(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 June 2001 (21.06.2001)

PCT

(10) International Publication Number
WO 01/45378 A1

(51) International Patent Classification⁷: H04M 11/04

(21) International Application Number: PCT/US00/33626

(22) International Filing Date: 8 December 2000 (08.12.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/172,706 16 December 1999 (16.12.1999) US
60/188,041 9 March 2000 (09.03.2000) US

(71) Applicant: ALPHA SYSTEMS LABORATORY [US/US]; 17712 Mitchell North, Irvine, CA 92612 (US).

(72) Inventor: PHAN, Mihn, V.; 25852 Desert Trail, Laguna Hills, CA 92653 (US).

(74) Agent: HACKLER, Walter, A.; 2372 S.E. Bristol, Suite B, Newport Beach, CA 92660 (US).

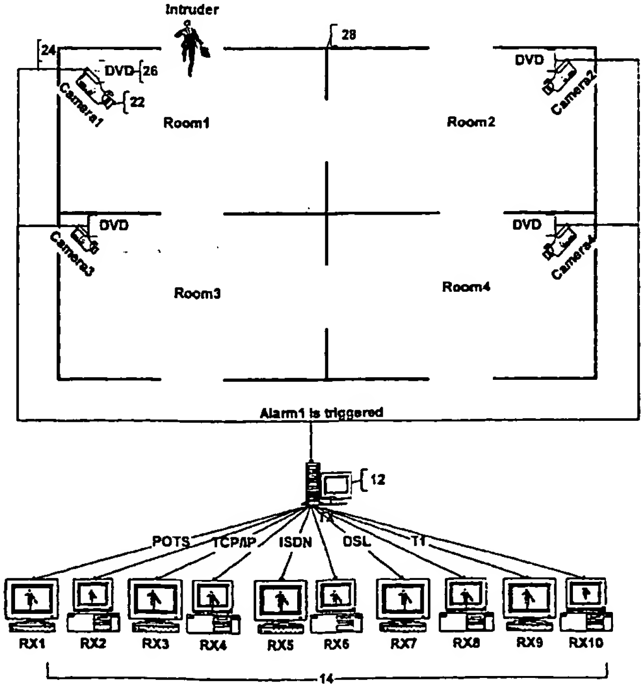
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR REMOTE INTERACTIVE MANAGEMENT OF A SURVEILLANCE DEVICE



(57) Abstract: Central transmitter (12) simultaneously communicates with a plurality of remote stations (14) through a variety of suitable connections, including but not limited to an analog telephone line, cellular or a higher-speed line such as an ISDN (integrated service digital network)

[Continued on next page]

WO 01/45378 A1

— *With amended claims and statement.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

line, T-1 or T-3 circuit, TCP/IP, XDSL or frame relay circuit. A recorder (26) is utilized to capture the output signals (24) from video cameras (22) positioned at remote receivers. A recording is thus provided directly into the hard disk of a microprocessor associated with recorder (26) at a remote receiver (28), thus eliminating the need to replace tapes associated with conventional video tape recording since subsequent recording override predetermined times of recording. Remote interactive management system provides for broadcast, sequential and only once notification of potential security breaches for both central transmitter (12) and remote stations (14). The remote backup system also provides a multi-threaded design allowing multiple connections between receiver units and transmitter units for facilitating backup. A receiver unit provides for automatic backup when a transmitter unit having a wireless antenna provides a signal that falls within a range of detection associated with the receiver unit. System and method also provide for video delay of information being sent from one entity to another, thus allowing for a live video signal to be delayed for a predetermined period of time.

SYSTEM AND METHOD FOR REMOTE INTERACTIVE MANAGEMENT OF A SURVEILLANCE DEVICE

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates generally to surveillance systems and more particularly to a method and apparatus for remote interactive management technology for surveillance systems.

2. Description of the Prior Art

Conventional surveillance systems are utilized to monitor fixed and moving sites such as, for example, buildings, commercial establishments, vehicles and other things that may be exposed to risk or peril. Typically, a central station communicates with a number of remote locations which each include monitoring equipment, such as video monitors, door and window alarms, motions detectors, microphones, fire detectors and the like. The monitoring equipment at the remote locations collects information relating to the security status of the facility being monitored. This information is then transmitted, typically via a phone line, to the central location where the security information from the remote locations is monitored.

Most modern surveillance systems, as noted above, rely upon video cameras mounted at remote locations for visually monitoring areas of concern. In particular, video cameras are typically mounted at risk sensitive areas such that they can record the signals and provide a video record for the past period of time in case any problems arise. Time lapse video cassette recorders (VCRs), which rely on slow motion taping, allow for a predetermined, limited period of recording per tape, for example twenty-four hours. Because the tape has a limited period of recording time, the effectiveness of the surveillance system is largely dependent upon whether the tape is changed once the tape's recording time period has elapsed. Typically, in operation, this means an operator must change the tape every day else no recording would be made and the surveillance systems compromised.

Conventional video surveillance systems also suffer from latency problems associated with detection. For example, when a security breach occurs at a remote location equipped with video and slow motion taping, the tape must be retrieved, sealed and sent to security authorities for review. This time delay between the security breach and tape review could be days. Moreover, modern systems do not allow a plurality of viewers to monitor video surveillance at remote locations. For example, while personnel at a central station are able to monitor remote locations, third parties, such as managers, police authorities and so forth, positioned elsewhere are not able to view what is going on. Consequently, communication regarding the security breach between interested parties is compromised.

Another problem associated with the security industry is the inability to effectively distinguish between true and false alarms, attributed in part to video cameras having limited ranges of view. For example, cameras are typically mounted to hone in on risk sensitive areas such as doors, windows and so forth. When an alarm condition occurs at a location outside of the cameras view, the central monitoring station is unable to determine whether the alarm if true or false. Consequently, because of the frequency of false alarms and the inability to verify whether such alarms are true or not, authorities are often slow to respond.

What is needed therefore is an apparatus and method for providing a surveillance system that minimizes the risk of human error, is accessible by a plurality of parties, and effective.

SUMMARY OF THE INVENTION

The present invention provides a method and apparatus for remote interactive management of a surveillance system. Central transmitter simultaneously communicates with plurality of remote receiver through a variety of suitable connections, including but not limited to an analog telephone line, cellular or a higher-speed line such as an ISDN (integrated services digital network) line, T-1 or T-3 circuit, TCP/IP, XDSL or frame relay circuit. A recorder, such as a digital video disk recorder (DVD) or VCR, is utilized to capture the output signals from video cameras positioned at remote receivers. A recording is thus provided directly into the hard disk of a microprocessor associated with the recorder at the remote receiver, thus eliminating the need to replace tapes associated with conventional video tape recording since subsequent recordings override predetermined times of recording. Remote interactive management system provides for broadcast, sequential and only once notification of potential security breaches for both central transmitter and remote stations. The remote backup system also provides a multi-threaded design allowing multiple connections between receiver units and transmitter units for facilitating backup. The receiver unit provides for automatic backup when a transmitter unit having a wireless antenna provides a signal that falls within a range of detection associated with the receiver unit. The present invention also provides for video delay of information being sent from one entity to another, thus allowing for a live signal to be delayed for a predetermined period of time.

The present invention provides, in a first aspect, a surveillance system for conducting surveillance on a plurality of sites in a network, including a monitoring unit for transmitting and receiving data from and to the sites in the network, a communication device for connecting the sites and the monitoring unit in the network, and a processor associated with the central monitoring unit for managing communications between the monitoring unit and the sites in the network.

In another aspect, the present invention provides a method for conducting surveillance on a plurality of sites in a network, including the steps of transmitting and receiving data from and to the sites in the network using a monitoring unit and substantially simultaneously communicating with the sites in the network, connecting the sites and the monitoring unit in the network, and managing communications between the monitoring unit and the sites in the network.

These and other features and advantages of this invention will become further apparent from the detailed description and accompanying figures that follow. In the figures and description, numerals indicate the various features of the invention, like numerals referring to like features throughout both the drawing figures and the written description.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of a remote interactive management system implemented on a transmitter server station in communication with a plurality of remote receiver stations in accordance with the present invention.

FIG. 2 is a block diagram of a remote interactive management system implemented on a receiver in communication with a plurality of transmitter server stations in accordance with the present invention.

FIG. 3 is block diagram of the DVD and alarm features of the remote interactive management system.

FIG. 4 is a flowchart of a method for providing notification of a security breach including broadcast, sequential and once only modes.

FIG. 5 is a detailed block diagram of the broadcast notification mode shown in FIG. 4.

FIG. 6 is a detailed flowchart of the broadcast notification mode shown in FIG. 5.

FIG. 7 is a detailed block diagram of the sequential notification mode shown in FIG. 4.

FIG. 8 is a detailed flowchart of the sequential notification mode shown in FIG. 7.

FIG. 9 is a detailed flowchart of the only once mode shown in FIG. 4.

FIG. 10 is a block diagram of a remote backup system in accordance with the present invention.

FIG. 11 is a block diagram of the interactions between transmitter and receiver units in remote backup mode shown in FIG. 10.

FIG. 12 is a flow chart of transmitter unit operation in remote backup system shown in FIG. 10.

FIG. 13 is a detailed flow chart of one method for waiting for a connection, as shown in FIG. 12.

FIG. 14 is a detailed flow chart of one method for creating a thread to do backup, as shown in FIG. 12.

FIG. 15 is a detailed flow chart of one method for determining whether to abort a program, as shown in FIG. 12.

FIG. 16 is a detailed flow chart of the transmitter unit operation in remote backup system as shown in FIG. 12.

FIG. 17 is a flow chart of the receiver unit operation in remote backup system shown in FIG. 10.

FIG. 18 is a detailed flow chart of one method for scanning for valid target units, as shown in FIG. 17.

FIG. 19 is a detailed flow chart of one method for creating a thread to execute backup procedures, as shown in FIG. 17.

FIG. 20 is a detailed flow chart of a method for determining whether to abort the backup program, as shown in FIG. 17.

FIG. 21 is a block diagram of a general network layout of one video pass thru configuration in accordance with the present invention.

FIG. 22 is a detailed flow chart of a method for providing video pass thru in remote interactive management system shown in FIG. 21.

FIG. 23 is a detailed flow chart of a method for checking for incoming mail, as shown in FIG. 22.

FIG. 24 is a detailed flow chart of a method for checking for outgoing mail, as shown in FIG. 22

FIG. 25 is a flow chart of one method for interpreting incoming mail, as shown in FIG. 22.

FIG. 26 is a flow chart of one method for interpreting outgoing mail, as shown in FIG. 22.

FIG. 27 is an illustrative block diagram of the video delay feature in accordance with the present invention.

FIG. 28 is a flow chart of one method for providing video delay.

FIG. 29 is a general block diagram of a routine for eliminating a user's interaction on maintaining capacity for the recording module.

FIG. 30 is a block diagram of a routine for maintaining capacity for a recording module.

FIG. 31 is flow chart of a routine for enacting load settings shown in FIG. 30.

FIG. 32 is a flow chart of a routine for checking all drives detected as shown in FIG. 30.

FIG. 33 is a general block diagram of a routine for a user to automatically establish and terminate connections with receivers and/or transmitters the user is monitoring at any desired time.

FIG. 34 is a flow chart of a routine for initialization as shown in FIG. 33.

FIG. 35 is a flow chart of a routine for performing work related to site touring as shown in FIG. 33.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT(S)

The present invention provides for remote interactive management of a surveillance system. Referring to FIG. 1, remote interactive management system 10 implemented on central transmitter 12 in communication with a plurality of remote receivers 14 is illustrated. Central transmitter 12 includes at least one transmitter and server computer 16 on which information is stored and from which remote receivers 14 and/or clients can retrieve that information. Each remote receiver 14 may include a computer including display terminal 18 for retrieving information from server computers 16, entering data, and performing other surveillance related tasks.

Central transmitter 12 simultaneously communicates with plurality of remote receiver 14 through a variety of suitable connections, including but not limited to an analog telephone line, cellular or a higher-speed line such as an ISDN (integrated services digital network) line, T-1 or T-3 circuit, TCP/IP, XDSL or frame relay circuit. In particular, for example, remote receiver 14 communicates with central transmitter 12 utilizing an analog modem over a switched dial-up telephone line. This line may be a plain old telephone service (POTS) line, typically at a speed of 56Kbps, although one skilled in the art will recognize that any viable transmission speed may be utilized. Remote receiver 14 may also communicate with central transmitter 12 via an ISDN adapter that connects over a switched digital telephone line. In another configuration, remote receiver 14 communicates with central transmitter 12 via a synchronous serial interface utilizing a frame relay standard over a high-speed leased digital line such as a T-1 or T-3 line. Communication may also take place between remote receiver 14 and central transmitter 12 using existing cable television network lines. In this case, remote receiver 14 may have a cable modem for connecting to the central transmitter. Moreover, remote client can communicate with central transmitter 12 over a Transmission Control Protocol/Internet Protocol (TCP/IP) connection. For example, remote receiver generates a Hypertext Transfer Protocol (HTTP) request for information associated with surveillance on a particular store, and a TCP/IP connection is then established between the remote receiver 14 and central transmitter 12. One skilled in the art will recognize that the present invention is not limited to the particular transmission means identified herein but rather other suitable and newly developed transmission means can be utilized as well.

As a result of the simultaneous communication with a plurality of remote receivers 14 utilizing a variety of connection means, remote interactive management system 10 of the present invention advantageously facilitates communication between remote receivers 14 and central transmitters 12 such that the latter can not only monitor remote receivers 14, but remote receivers 14 can correspondingly simultaneously communicate with central transmitter 12 as well as each other, as explained in detail below.

Referring to FIG. 2, a further aspect of remote interactive management system 20 is illustrated. Each remote receiver 14 may communicate with a plurality of central transmitters 12 simultaneously to receive live video and control all of the central transmitters 12 simultaneously. As with the configuration 10 illustrated in FIG. 1, remote receiver 14 may communicate with central transmitters 12 through a variety of suitable connections, including but not limited to an analog telephone line, cellular or a higher-speed line such as an ISDN (integrated services digital network) line, T-1 or T-3 circuit, TCP/IP, XDSL or frame relay circuit. In a typical configuration, remote receiver 14 communicates with as many as sixteen different central transmitters 12. Remote receiver 14 is able to view all of the central transmitters 12 it is in communication with simultaneously on the same display screen, thus saving cost and time in switching between receivers 14. Thus, in accordance with the present invention, remote interactive management system 20 minimizes the cost of having different receivers 14 for each transmitter 12 and to be able to reuse old communication devices. Since remote interactive management system 20 is able to connect to a plurality of different sites at once, the user can be more productive by concentrating on one monitor that is able to monitor the different sites than to focus on the monitors that represent the different sites.

Digital Video Recording

Referring to FIG. 3, remote interactive management system 10 and 20 illustrated in FIGS. 1 and 2 is preferably implemented utilizing digital video recording, thus providing a surveillance system that minimizes the risk of human error, is accessible by a plurality of parties, and effective in recording a standardized period of time. In particular, video cameras 22 are typically mounted at risk sensitive areas such that they can record the signals and provide a video record for the past period of time in case any problems arise. The output signals 24 are routed by control circuitry to a DVD 26 disposed at remote receiver 28. In accordance with the preferred embodiment of the invention, a DVD 26 is utilized to capture the output signals 24 from the video cameras 22. A recording is thus provided directly into the hard disk of the microprocessor associated with DVD 26 at remote receiver 28, thus eliminating the need to replace tapes associated with conventional video tape recording since subsequent recordings override predetermined times of recording. For example, after recording the signals captured from video cameras 22 over a length of time, such as twenty-four hours, subsequent recordings sequentially override what already has been recorded. One skilled in the art will recognize that the length of time available for recording is not limited by only the particular specifications of the DVD 26 in use. The effectiveness of the surveillance system is thus no longer dependent upon whether a tape is changed once it's recording time period has elapsed.

In accordance with the present invention, the use of a DVD 26 also minimizes latency problems associated with detection. For example, when a security breach occurs at remote receiver 28 equipped with video camera 22 and DVD 26, central transmitters 12 or other remote receivers 14 can, via the a particular communication path as described in FIGS. 1 and 2 remotely and automatically view the video clip, rather than wait for it to be retrieved and shipped. Remote receivers 14 and central transmitters 12 can thus monitor activity at remote receiver 28. In operation, typically, third parties, such as managers, police authorities and so forth, positioned elsewhere from remote receiver 28 can monitor activity at remote receiver 28 as long as they are in communication with central transmitter 12 connected to remote receiver 12. One skilled in the art will recognize that the present invention is not limited to the use of a DVD, rather a conventional analog or digital VCR may be used as well.

Remote Interactive Alarm

As shown in FIG. 3, output signals 24 from each video camera 22 are routed by control circuitry to a DVD 26 disposed at remote receiver 28. Each video camera 22 is mounted such that it can be adjusted in accordance with control signals 30 from central transmitter 12 or any of remote receivers 14 in communication with remote receiver 28 through central transmitter 12. Consequently, central transmitter 12 and other remote receivers 14 can individually send control signals 30 to adjust the position of video camera 22 at remote receiver 28. Moreover, video cameras 22 can be remotely automatically adjusted in response to motion detection of security breaches. For example, in accordance with detection of motion at a door, video camera 22 automatically adjusts its angle of view to the door from another area, such as a window, to continue recording a possible breach at the door. After video camera 22 is adjusted, a signal is automatically directed to central transmitter 12 indicating a possible security breach, thus allowing those at the central transmitter 12 to determine whether a security breach actually occurred. Thus, by providing automatic adjustment of video cameras 22 in response to direct central transmitter 12 or remote receiver 14, and/or motion detection, the present invention effectively distinguishes between true and false alarms. Consequently, because of the ability to verify whether such alarms are true or not, security personnel will be able to respond quickly.

Notification

Remote interactive management system provides for broadcast, sequential and only once notification of potential security breaches for both central transmitter and remote stations. FIG. 4 is a flowchart 32 of a method for providing notification of a security breach including broadcast, sequential and once only modes. One skilled in the art will recognize that the flowchart may be implemented in software, hardware or a combination thereof. Broadcast, sequential and only once notification modes are provided on remote interactive management system 10, with the user defining the desired notification mode. In particular, remote receiver 28 continuously checks for triggered inputs that are generated in response to security breaches that may include but are not limited to alarm notifications, detection mechanisms on doors and windows and so forth (step 34). In the case of a plurality of video cameras 22 disposed at remote receiver 14, remote receiver 14 determines the particular video camera 22 associated with the triggered input (step 36). Recording, if not already in operation, is implemented (step 38). A dial out procedure is then initiated to contact central transmitter 12 (step 40) and live video is sent thereto (step 42). Notification is then initiated by central transmitter 12 utilizing information stored in a database regarding the particular mode of notification required such that information can be provided to remote receivers 14 (step 44). Database information can include but is not limited to the particular IP addresses of remote receivers 14 as well as the procedures for dialing out to such addresses. Depending on the particular mode of operation determined by information in step 44, either broadcast (step 46), sequential (step 48) or only once (step 50) mode notification is initiated. Broadcast (step 46), sequential (step 48) and only once (step 50) modes are discussed in detail below. Notification is then sent to central transmitter 12, which then communicates the security breach and live video to the central transmitters 12 and remote receivers 14 in the same network configuration (step 52). Steps 34 through 52 are repeated until the triggered input indicating a security breach has been terminated (steps 54 and 56).

FIG. 5 is a detailed block diagram 58 of broadcast notification mode shown in FIG. 4. In particular, referring to FIG. 5, broadcast notification is illustrated utilizing, for example, an intruder 60 entering a four-room remote receiver 28 with each room being monitored by a video camera 22. Remote receivers 14 and 28 (receiver involving security breach) are in communication with central transmitter 12. When central transmitter 12 receives output signal 62 indicating a security breach, it simultaneously communicates the security breach to the remainder of the remote receivers 14 through any of a variety of suitable connections, including but not limited to an analog telephone line, cellular or a higher-speed line such as an ISDN (integrated services digital network) line, T-1 or T-3 circuit, TCP/IP, XDSL or frame relay circuit. In a typical operation, central transmitter 12 simultaneously communicates the security breach to 256 remote receivers 14 using mixed communication means.

Referring to FIG. 6, a detailed flowchart 64 of the broadcast notification mode shown in FIG. 5 is illustrated. During broadcast notification, all remote receivers 14 or other devices in communication with central transmitter 12 are notified simultaneously and immediately. As noted above, broadcast notification is implemented as an algorithm at central transmitter 12 upon notification from remote receiver 28 where a security breach has occurred. In particular, central transmitter 12 initially determines IP addresses for remote receivers 14 linked with remote receiver 28 where security breach has occurred (step 66). All of the IP addresses are then queued up for dialing out to remote receivers (step 68) at the same time. If the connection is not established, the central transmitter 12 continues its attempts to establish communication with remote receivers 14 for a predetermined number of times (steps 70 and 72). Once communication is established, central transmitter 12 sends out notification that a security breach has occurred at remote receiver 28, including providing access to live-video if desired (step 74). To facilitate immediate communication, a predetermined time for maintaining communication with remote receivers 14 may be specified, thus minimizing any communication congestion which may occur when a large number of remote receivers 14 is being notified (step 76). If a time is specified, central transmitter 12 terminates communication with remote receiver when the predetermined period of time has elapsed (steps 78 and 80). In the event that no predetermined termination time is specified, the central transmitter repeats steps 70-80 until the last remote receiver has been notified (step 82), upon which time the notification procedure is completed (step 84).

FIG. 7 is a detailed block diagram 86 of sequential notification mode shown in FIG. 4. In particular, referring to FIG. 7, sequential notification is illustrated utilizing the same intruder scenario as for broadcast notification. For example, an intruder 60 entering a four-room remote receiver 28, with each room being monitored by a video camera 22, triggers a security measure. After the security measure, such as an alarm, is triggered, remote receiver 28 notifies central transmitter 12 via connection 88. When central transmitter 12 receives notification indicating a security breach, it sequentially communicates the security breach to the remainder of the remote receivers 90, 92 and 94 through any of a variety of suitable connections over connections 96, 98 and 100, respectively.

In a typical embodiment, a user such as manager may be monitoring remote receiver 90. Upon termination of connection 96 by the user or expiration of connection 96 after a predetermined period of time has elapsed, transmitter 12 establishes a connection with the next remote receiver 92 over connection 98. A central user may be monitoring remote receiver 92. Finally, after the central user has logged off or the connection time has elapsed, central transmitter 12 establishes a connection with remote receiver 94 over connection 100.

In a typical operation, central transmitter 12 serially communicates the security breach to 256 remote receivers 14 using mixed communication means in a similar manner.

Referring to FIG. 8, a detailed flowchart 102 of the sequential notification mode shown in FIG. 7 is illustrated. During sequential notification, all remote receivers 14 (such as remote receivers 90, 92 and 94 shown in FIG. 7) or other devices in communication with central transmitter 12 are notified sequentially. As noted above, sequential notification is implemented as an algorithm at central transmitter 12 upon notification from remote receiver 28 where a security breach has occurred. In particular, central transmitter 12 initially determines IP addresses for remote receivers 14 linked with remote receiver 28 where security breach has occurred (step 104). One, as opposed to all in broadcast notification shown in FIG. 6, of the available IP addresses are then queued up for dialing out to remote receivers (step 106). Once communication is established (step 108), central transmitter 12 sends out notification that a security breach has occurred at remote receiver 28, including providing access to live-video if desired (step 110). To facilitate immediate communication, a predetermined time for maintaining communication with remote receivers 14 may be specified, thus minimizing any communication congestion which may occur when a large number of remote receivers 14 is being notified (step 112). If a time is specified, central transmitter 12 terminates communication with remote receiver when the predetermined period of time has elapsed (steps 114 and 116). In the event that no predetermined termination time is specified, the central transmitter repeats steps 104-116 until the last remote receiver has been notified (step 118), upon which time the notification procedure is completed (step 120).

Referring to FIG. 9, a detailed flowchart 122 of the once only notification mode shown in FIG. 4 is illustrated. During sequential notification, all remote receivers 14 or other devices in communication with central transmitter 12 are notified only once. As noted above, only once notification is implemented as an algorithm at central transmitter 12 upon notification from remote receiver 28 where a security breach has occurred. In particular, central transmitter 12 initially determines IP addresses for remote receivers 14 linked with remote receiver 28 where security breach has occurred (step 124). One, as opposed to all in broadcast notification shown in FIG. 6, of the available IP addresses are then queued up for dialing out to remote receivers (step 126). If the remote receiver is busy or cannot be accessed for any reason (step 128), central transmitter determines whether there are any more IP addresses (step 136) and then if so, attempts to establish communication with the IP address for the next remote receiver 14 (step 134). If no IP addresses are available (step 136), the once only notification process is terminated (step 146).

If, in step 128, central transmitter 12 is able to access remote receiver 14 and no failure has occurred (steps 130 and 132), central transmitter 12 sends out notification that a security breach has occurred at remote receiver 28, including providing access to live-video if desired (step 140). Once a predetermined period of time has elapsed (step 142), central transmitter 12 terminates communication with remote receiver (steps 144) and the once only notification procedure is completed (step 146).

In accordance with an advantage of the present invention, any of the three methods of notification can be alternatively implemented and the user can automatically switch from one method to the other.

Remote Backup

As is illustrated in FIG. 10, the remote backup system 148 of the present invention provides a multi-threaded design allowing multiple connections between receiver units 150 and 152 for backup and transmitter units 154, 156, 158 and 160. One skilled in the art will recognize that the multi-threaded design of the present invention provides various configuration options and that the particular option shown in FIG. 10 is for illustrative purposes only. Receiver units 150 and 152 provide back up for information including, but not limited to, video clips from transmitter units 154, 156, 158 and 160 and include ample storage for backing up multiple transmitter units. Transmitter units 154, 156, 158 and 160 record activities such as video or alarm recordings, operate as waiting units that accepts connections from receiver units 150 and 152, and transfers data to receiver units 150 and 152 upon requests.

As explained in detail below, remote backup feature of the present invention may be used in various applications for remote backup. For illustrative purpose, the present invention will be described in conjunction with receiver units 150 and 152 representing transportation hubs for busses and transmitter units 154, 156, 158 and 160 representing busses each having a wireless antenna for transmitting communication signals to the wireless antenna disposed at receiver units 150 or 152.

Referring to FIG. 11, a block diagram of the interactions between transmitter and receiver units in remote backup mode illustrated in FIG. 10 is shown. In accordance with the present invention, receiver unit 152 provides for automatic backup when a transmitter unit having a wireless antenna provides a signal that falls within a range of detection associated with receiver unit 152. For example, detection range of wireless receiver 172 of receiver unit 152 is shown within broken lines. Since wireless transmitter units 162 and 164 send signals that fall within the range, they receive automatic back up. In contrast, wireless transmitter unit 166 will not be automatically backed up until it enters the detection range wireless receiver 172.

The present invention also provides for backup when transmitters are hard wired connected to receiver unit 152. For example, transmitter units 168 and 170 are wired to receiver unit 152 and thus receive automatic backup even without falling within detection range of wireless receiver 172. Regular backup, in intervals 174 such as hourly, daily, weekly and monthly, are also provided to transmitter units, such as transmitter units 156, 158 and 160.

Referring to FIG. 12, a flow chart 178 of a method of operation for a transmitter unit in remote backup system 148 is illustrated. In particular, transmitter initially waits for a connection to be established with receiver unit (step 180) and then creates a thread to perform the backup procedure (step 182). The new created thread will run in the background to provide responses to the remote receiver unit, and will terminate itself when the task is completed. If no connection is established in step 180, the transmitter continues to monitor for one. Once a thread is created for backup (step 182), the determination is made whether to abort the program (step 184). If not, steps 180-184 are repeated. If the program is aborted, the method of operation is terminated (step 186).

Referring to FIG. 13, a flow chart 188 of a method for waiting for a connection, as shown in step 180 in FIG. 12, is illustrated. In particular, a transmitter initially listens for incoming connections with receiver unit (step 190). The transmitter then retrieves information from a database (step 192) to verify authorization of the user (step 194). If authorization is denied, steps 190-194 are repeated. Once authorization is provided, the method of operation is terminated (step 196).

Referring to FIG. 14, a flow chart 198 of a method for creating a thread to perform backup procedures, as shown in step 182 in FIG. 12, is illustrated. In particular, the thread for performing backup is initiated (step 200), lights associated with transmitter unit are turned on (step 202) and the transmitter unit waits for instructions from other remote receivers (step 204). Information from gathered from the transmitter, including but not limited to new files (step 206), modified files (step 208), new subdirectories (step 210), deleted files (step 212) and other functions (step 214) are marked for backup. In particular, new files and modified files are copied (step 216), new subdirectories are copied (step 218) and deleted files are purged (step 220). When the backup procedure is completed, the lights are turned off (step 222) and the thread terminated (step 224).

Referring to FIG. 15, a flow chart 198 of a method for determining whether to abort the backup program, as shown in step 184 in FIG. 12, is illustrated. In particular, if the user input indicates that the user wants to exit (steps 228 and 230), authorization for termination of the transmitter unit is checked (step 232) and permission is requested (step 234). Once granted, the backup procedure is terminated (step 236). However if the user does not want to exit (step 230), the program continuously loops to step 228 to retrieve more input from the user. If permission for exit is checked and subsequently denied (step 234), the program returns to step 228 to continue to receive input from the user.

Referring to FIG. 16, a detailed flow chart 238 of the method of operation for the transmitter unit in remote backup system 148 is illustrated. In particular, the transmitter initially listens for incoming connections (step 240) and then retrieves information from its database (step 242). Authorization is then checked to determine whether such information could be backed up (step 246). If authorization is not granted, the transmitter returns to listening for incoming connections (step 240). If authorization is granted, a new process to respond to the remote backup instructions is granted (step 248) and the transmitter signals the thread to start working (step 250). If the user has not terminated the transmitter unit (step 252), steps 240-252 are repeated. If the user has terminated the transmitter unit (sep 254), the method is terminated (step 254).

Referring to FIG. 17, a flow chart 256 of a method of operation for a receiver unit in remote backup system 148 is illustrated. In particular, receiver initially scans for valid target units (step 258) and then creates a thread to perform the backup procedure if a valid unit is found (step 260). The new created thread will run in the background to provide responses to the remote receiver unit, and will terminate itself when the task is completed. If no valid target is found in step 258, the receiver continues to scan for one. Once a thread is created for backup (step 260), the determination is made whether to abort the program (step 262). If not, steps 258-262 are repeated. If the program is aborted, the method of operation is terminated (step 264).

Referring to FIG. 18, a flow chart 266 of a method for scanning for valid target units, as shown in step 258 in FIG. 17, is illustrated. In particular, the receiver initially scans for valid transmitter units (step 268). If a connection is established (step 274), receiver retrieves data from the remote transmitter unit (step 276) and verifies that the unit is a target unit (step 278). If in step 268, scanning results in no valid units, the method checks for any schedule that is triggered (step 270) before it is terminated (step 282). If there is a schedule triggered, the IP address is added to the scanning list before the method is terminated (step 282). Likewise, if in step 278 the unit detected is not a target unit, the method is terminated (step 282).

Referring to FIG. 19, a flow chart 284 of a method for creating a thread to execute backup procedures, as shown in step 260 in FIG. 17, is illustrated. In particular, the thread for performing backup is initiated (step 268), lights associated with transmitter unit are turned on (step 288) and the receiver unit waits checks for files and directories (step 290). Information from gathered from the transmitter, including but not limited to new files (step 292), modified files (step 294), new subdirectories (step 296), deleted files (step 298) and other functions (step 300) are marked for checked. In particular, new files and modified files are copied (step 302), new subdirectories are copied (step 304) and deleted files are purged (step 306). When the backup procedure is completed, the lights are turned off (step 308) and the thread terminated (step 310).

Referring to FIG. 20, a flow chart 198 of a method for determining whether to abort the backup program, as shown in step 262 in FIG. 17, is illustrated. In particular, IP addresses stored in the database are initially retrieved (step 316) and all IP addresses that need to be scanned are added (step 318). The receiver unit then scans for valid units (step 320). If there are no valid units (step 320), the receiver unit determines whether any schedule is triggered (step 324) and if so, adds the IP address to the scanning list before checking for user termination (step 340). If there are valid units (step 320), a connection is established (step 326) and data from the remote transmitter unit is retrieved (step 328). If the unit is not a target unit (step 330), the connection is aborted and terminated if desired by the user (step 340). However, if the remote unit is a target unit (step 330), a new process to execute the backup is created (step 332). The process if told what needs to be done to accomplish backup (step 334) and the process starts working (step 336). The user provides input for termination of the process (step 340). If not, the process repeats steps 320-340.

Video Pass Thru

Referring to FIGS. 1 and 2, as a result of the simultaneous communication with a plurality of remote receivers 14 utilizing a variety of connection means, remote interactive management system 10 of the present invention advantageously facilitates communication between remote receivers 14 and central transmitters 12 such that the latter can not only monitor remote receivers 14, but remote receivers 14 can correspondingly simultaneously communicate with central transmitter 12 as well as each other, as explained in detail below. The present invention thus provides with both direct and indirect communication between both central transmitters and remote receivers within the same communication link, regardless of the type of connection. In particular, as noted above, central transmitter 12 simultaneously communicates with plurality of remote receiver 14 through a variety of suitable connections, including but not limited to an analog telephone line, cellular or a higher-speed line such as an ISDN (integrated services digital network) line, T-1 or T-3 circuit, TCP/IP, XDSL or frame relay circuit.

The present invention thus provides video pass thru allowing both direct and indirect communication among transmitters and receivers. For example, when a security breach occurs at remote receiver 28 equipped with video camera 22 and DVD 26, central transmitters 12 or other remote receivers 14 can, via the a particular communication path as described in FIGS. 1 and 2 remotely and automatically view the video clip, rather than wait for it to be retrieved and shipped. Remote receivers 14 and central transmitters 12 can thus monitor activity at remote receiver 28. In operation, typically, third parties, such as managers, police authorities and so forth, positioned elsewhere from remote receiver 28 can monitor activity at remote receiver 28 as long as they are in communication with central transmitter 12 connected to remote receiver 12.

Referring to FIG. 21, general network layout 346 of one video pass thru configuration is illustrated. Data of transmitter 346 is sent to transmitter 348 by using receiver 344 as a message pass-on station. Therefore, the message will be sent from transmitter 346 to receiver 344. When receiver 344 receives the message, it will send the message to transmitter 348 in accordance with the methods discussed below. Referring to FIG. 22, a flow chart 350 of a method of operation for providing video pass thru in remote interactive management system is illustrated. In particular, the present invention checks for incoming data (step 352) and if there is data (step 354), the data is interpreted (step 356). If there is no incoming data (step 354), step 354 is skipped. In step 358, the present invention checks for outgoing data and if there is data (step 360), the data is interpreted (step 362). Steps 352-364 are repeated until the process is stopped (step 364) whereupon the process is terminated (step 366).

Referring to FIG. 23, a flow chart 368 of a method for checking for incoming mail, as shown in step 368 in FIG. 22, is illustrated. In particular, the process initially checks for a valid connection (step 370) and if none is found (step 372), the process is terminated (step 382). However, if a valid connection is found (step 372), the buffer is checked for incoming data (step 374) and if data is present (step 376), the data is packed (step 378) and dispatched (step 380). If data is not present in the buffer (step 376), the process is terminated (step 382).

Referring to FIG. 24, a flow chart 384 of a method for checking for outgoing mail, as shown in step 358 in FIG. 22, is illustrated. In particular, the process initially checks the outgoing queues for mail (step 386). If a queue is found (step 388), the queue is extracted and dispatched (step 392). The process is then terminated.

Referring to FIG. 25, a flow chart 396 of a method for interpreting incoming mail, as shown in step 356, in FIG. 22, is illustrated. In particular, the process initially determines whether the packet is a pass thru packet (step 400). If so (step 402), the next destination is determined (step 406) and the site is checked to make sure it is valid (step 408). If it is valid (step 410), the packet is sent out (step 412) and the process is then terminated (step 414). If the packet is not a pass thru packet (step 402), the packet is dispatched normally (step 404) and the process is then terminated (step 414).

Referring to FIG. 26, a flow chart 416 of a method for interpreting outgoing mail, as shown in step 362, in FIG. 22, is illustrated. In particular, the process initially determines whether the packet is a pass thru packet (step 420). If so (step 422), the network topology is retrieved (step 426) and the shortest and fastest path is computed (step 428). If the path is found (step 430), the path information is added into the packet to be delivered (step 432). The packet is then sent (step 434) and the process is terminated (step 436). If in step 422 the packet is not for pass thru, the packet is dispatched normally (step 424).

Video Delay

Referring to FIG. 27, the present invention provides for video delay of information being sent from one entity to another, thus allowing for a live signal to be delayed for a predetermined period of time. For example, when a security breach 420 occurs at remote receiver 424 equipped with video camera 422, monitors 426 and 428 or other remote receivers can, via the a particular communication path as described in FIGS. 1 and 2 remotely and automatically view the video clip, rather than wait for it to be retrieved and shipped. Monitor 426 provides live video while monitor 228 provides a delay of the live video shown on monitor 426. Users can thus actively view both monitors and rely on delayed video monitor 428 to confirm security breaches. In particular, referring to FIG. 28, a flow chart 430 of a method for providing video delay is illustrated. The video image captured (step 432) is displayed on the image of the first monitor (step 434) and the video image is saved to disk and/or memory on the computer associated with the output signal from video camera 422 (step 436). The image that was captured is then retrieved for redisplay on another monitor (steps 438 and 440). If the procedure is not terminated (step 442), steps 432-442 are repeated.

File Checker

Referring to FIG. 29, the present invention provides for eliminating a user's interaction on maintaining capacity, such as disk space, for the recording module utilized as discussed above. In particular, a file checker automatically deletes the oldest video clips to make room for a new one and determines which drive the new file should be created on. While the video clip is being created, the file checker is also running in the background to ensure there is enough disk space for the recording. As illustrated in the recording module 446 shown in FIG. 29, a file checker 448-456 is created for each individual module, which may include but is not limited to, events 448, R.O.D. 460, ATMs 462-462 and other instances 466.

Referring to FIG. 30, general block diagram of a routine 468 for maintaining capacity for a recording module is illustrated. In particular, after initiation of the routine (step 470), load settings are initiated (step 472, discussed in detail in FIG. 31) and the disk space is checked (step 474). In the case of an error, for example, no space is detected, drives are not detected or operational or some other related problem, routine 468 is terminated. Assuming that drives are detected (step 474), all the available drives are checked for disk space (step 478). For each drive, routine 468 determines whether there is enough space (step 480). If so, no deletion of video clips is required at the time and routine 446 continues running in the background to ensure there is enough disk space for recording (step 482).

On the other hand, if there is not enough space detected, routine 468 finds the oldest file recorded (step 484) and sends a command to delete the file (step 486). Routine 468 then determines whether the file was actually deleted (step 488). If not, routine 468 instructs the module to delete the file (step 490) and returns to finding the oldest file (step 484). If the file is actually deleted (step 488), routine 468 determines whether the current drive as enough space after deletion (step 492). Whether the current drive has enough space after deletion depends on the user's predetermined input regarding what space is required for new video clips. This variable could be changed in accordance with the user's particular needs. Assuming there is enough space (step 494), no further deletion of video clips is required at the time and routine 446 continues running in the background to ensure there is enough disk space for recording (step 482). If routine 468 determined that there is not enough space even after deletion (step 494), routine 468 repeats steps 484-494.

Referring to FIG. 31, a detailed flow chart of a routine 496 for enacting load settings, as shown in step 472, in FIG. 30, is illustrated. After initiation of routine 496 (step 498), database is opened (step 500), and information regarding the drives and paths utilized is located (step 502). For example, a typical drive and path may be characterized as "c:/Recording/Events". The drives and paths located are then checked (step 504) to determine whether drive(s) are valid (step 506), a new drive exist (step 508) or there were modifications in the drive identification since the last time routine 496 was executed (step 510). In particular, if a drive is determined to be invalid (step 506), routine 516 is terminated. If a new drive is found since the last time routine 496 was executed (step 508), the new drive is prepared for use if desired (step 512). Routine 516 is then terminated (step 516). If there were modifications in the drive identification, such as the drive letter, since the last time routine 496 was executed (step 510), the drive is reconfigured for use (step 514) and routine is then terminated (step 516). A modification in the drive identification can be caused by, but is not limited to, switching removable hard drives or mapping/unmapping shared drives may affect the drive letter.

Referring to FIG. 32, a detailed flow chart of a routine 518 for checking all drives detected, as shown in step 478, in FIG. 30, is illustrated. After routine 518 is initiated, it is determined whether there is a drive to check (step 522). If not, routine is terminated (step 530). If there is a drive, it is checked for available space (step 524) and if there is enough space (step 526), routine 518 is terminated (step 530). If there is not enough available space, the next drive is located (step 528) and routine 518 returns to step 524, where the drive is checked (step 524).

Site Touring

Referring to FIG. 33, the present invention provides a routine 532 for a user to automatically adjusts, establish and terminate connections with receivers and/or transmitters the user is monitoring at any desired time. In particular, referring to FIG. 1, the present invention is particularly useful when applied to remote interactive management systems 10 which are implemented on central transmitter 12 in communication with a plurality of remote receivers 14. In such cases, the user may desire an automatically method for adding or removing from certain receivers from the plurality being monitored. In cases where a user is monitoring hundreds of store sites, being able to add or remove a particular site without physically having to go to the location or implement a variety of measures is particularly advantageous. In accordance with an advantage of the invention, this allows a user no longer have to interact with programs implementing such surveillance measures that are no longer desired. For example, the user may monitor hundreds of sites without touching the keyboard and/or mouse.

Referring to FIG. 33, after routine 532 is initialized (step 534), it checks for triggered events established by the user that would cause the surveillance connection to be established or terminated (step 536). Such triggered events could include, but are not limited to, user's desire to terminate monitoring sites that are closed down and no longer need monitoring, user adding surveillance for additional sites developed, and so forth. One skilled in the art will recognize that the present invention is not limited to any particular means of triggering establishing or terminating connections between the user monitoring and the device to be monitored. If there are no events triggered, user inputs are checked (step 546). If no user inputs are detected, work related to site touring is performed in accordance with step 548, discussed in detail in FIG. 33. If routine 532 is terminated (step 550), routine is stopped (step 552). If not, routine 532 returns to step 536, where it checks for triggered events.

If in step 546, routine 532 detects one or more user inputs, the surveillance information is manipulated according to user choice. Such choices can include, but are not limited to, the surveillance information being played back (step 538), skipped (step 540), stopped (step 542) or paused (step 544). Thereafter, if routine 532 is terminated (step 550), routine is stopped (step 552). If not, routine 532 returns to step 536, where it checks for triggered events.

If in step 536, one or more triggered events are detected, surveillance information is at a minimum played back to the user for monitoring. Thereafter, if routine 532 is terminated (step 550), routine is stopped (step 552). If not, routine 532 returns to step 536, where it checks for triggered events.

Referring to FIG. 34, a detailed flow chart of a routine 554 for initialization, as shown in step 534 in FIG. 33, is illustrated. One skilled in the art will recognize that database includes a collection of data stored together in or more computerized files, with each item being identifiable and retrievable by the user. As discussed in detail below, information stored in database may include, but is not limited to, schedule information related to surveillance (step 558) and information related to the group of sites monitored (step 560). The group information includes information such as site names, ips or phone numbers, number of retries and termination times. After storage, site information is retrieved (step 562) and routine 566 terminated (step 564).

Referring to FIG. 35, a detailed flow chart of a routine 566 for performing work related to site touring 548, as shown in step 548 in FIG. 33 is illustrated. Routine 566 initially determines whether the surveillance site (i.e. receivers or transmitters) touring feature is active or not (step 568). If activated, the next surveillance site among the plurality of sites being monitored is retrieved (step 576) and a new connection with that surveillance site requested (step 578). Thereafter, routine 566 is terminated (step 574).

If the surveillance site touring feature is not active, routine 566 determines whether a connection to a surveillance site has been established (step 570). If so, the new surveillance site located is initialized and thereafter, routine 566 is terminated (step 574). If no connection to a surveillance site has been established, routine 566 determines whether certain flags are present (step 572). Such flags could include, but are not limited to, instructions related to play (step 582), next (step 584), stop (step 586) and pause (step 588). In particular, for the "play" instruction, routine 566 makes the current group of surveillance sites active (step 582). For the "next" instruction, the current surveillance site is skipped (step 584). For the "stop" instruction, the current surveillance group of sites is stopped. For the "pause" instruction, the current surveillance group is paused. Thereafter, routine 566 is terminated (step 574).

Having now described the invention in accordance with the requirements of the patent statutes, those skilled in the art will understand how to make changes and modifications in the present invention to meet their specific requirements or conditions. Such changes and modifications may be made without departing from the scope and spirit of the invention as set forth in the following changes.

WHAT IS CLAIMED IS:

1. A surveillance system for conducting surveillance on a plurality of sites in a network, comprising:

a monitoring unit for transmitting and receiving data from and to said sites in said network;

a communication device for connecting said sites and said monitoring unit in said network; and

a processor associated with said central monitoring unit for managing communications between said monitoring unit and said sites in said network.

2. The system claimed in claim 1, wherein said monitoring unit substantially simultaneously communicates with said sites in said network.

3. The system claimed in claim 1, wherein said communication device comprises a variety of connections.

4. The system claimed in claim 3, wherein said connection includes an analog telephone line.

5. The system claimed in claim 3, wherein said connection includes a cellular line.

6. The system claimed in claim 3, wherein said connection includes an ISDN line.

7. The system claimed in claim 3, wherein said connections includes a T-1 line.

8. The system claimed in claim 3, wherein said connections includes a T-3 line.

9. The system claimed in claim 3, wherein said connections includes a TCP/IP line.

10. The system claimed in claim 3, wherein said connections includes a XDSL line.

11. The system claimed in claim 3, wherein said connections includes a frame relay circuit.

12. The system claimed in claim 1, further comprising a plurality of monitoring units, wherein at least one of sites substantially simultaneously communicates with said monitoring units.

13. The system claimed in claim 1, wherein said sites communicates with one another via said monitoring unit.

14. The system claimed in claim 1, further comprising:

a recorder in communication with each of site sites for recording surveillance data at said sites.

15. The system claimed in claim 14, wherein said recorder is a digital recorder.

16. The system claimed in claim 14 wherein each of said sites in said network can adjust said position of said recorder in any other site.

17. The system claimed in claim 14 wherein each of said monitoring units in said network can adjust said position of said recorder in any other site.

18. The system claimed in claim 1, wherein said monitoring unit provides notification to said sites in said network.

19. The system claimed in claim 18, wherein said notification is broadcast to said sites in said network.

20. The system claimed in claim 18, wherein said notification is sequentially transmitted to said sites in said network.

21. The system claimed in claim 18, wherein said notification is provided on a once only basis to said sites in said network.

22. The system claimed in claim 18, wherein said form of communication automatically adjusts based on user preference.

23. The system claimed in claim 22, wherein said instructions for adjustment are predefined in a database associated with said monitoring unit.

24. The system claimed in claim 1, wherein said monitoring unit backs up said surveillance data in response to said sites detected within a predetermined area.

25. The system claimed in claim 24, wherein said monitoring unit backs up said surveillance data in response to detection of signals associated with said sites when said sites enter a predetermined range.

26. The system claimed in claim 1, wherein delay of surveillance is delayed for a predetermined period of time.

27. The system claimed in claim 1, further comprising:

a file checker for automatically deleting surveillance information to create capacity for recording of recent surveillance information.

28. The system claimed in claim 27, wherein said surveillance information is recorded on video tape.

29. The system claimed in claim 1, further comprising means for automatically adjusting communications with said plurality of sites.

30. The system claimed in claim 29, wherein said adjusting communications comprises establishing and terminating communications with sites.

31. A method for conducting surveillance on a plurality of sites in a network, comprising the steps of:

transmitting and receiving data from and to said sites in said network using a monitoring unit and substantially simultaneously communicating with said sites in said network;

connecting said sites and said monitoring unit in said network; and

managing communications between said monitoring unit and said sites in said network.

32. The method claimed in claim 31, further comprising the step of transmitting and receiving data from and to said sites in said network using a plurality of monitoring units and substantially simultaneously communicating with said sites in said network

33. The method claimed in claim 31, wherein said sites communicate with one another via said monitoring unit.

34. The method claimed in claim 31, further comprising the step of:

recording surveillance data at said sites.

35. The method claimed in claim 34, wherein said recorder is a digital recorder.

36. The method claimed in claim 34, further comprising the step of:

said sites in said network adjusting said position of said recorder in any other site.

37. The method claimed in claim 34, further comprising the step of:

said monitoring units in said network adjusting said position of said recorder in any other site.

38. The method claimed in claim 31, further comprising the step of:

providing notification to said sites in said network using said monitoring unit.

39. The method claimed in claim 38, wherein said step of providing notification to said sites in said network using said monitoring unit further comprises the step of:

broadcasting said notification to said sites in said network.

40. The method claimed in claim 38, wherein said step of providing notification to said sites in said network using said monitoring unit further comprises the step of:

sequentially transmitting notification to said sites in said network.

41. The method claimed in claim 38, wherein said step of providing notification to said sites in said network using said monitoring unit further comprises the step of:

providing notification on a once only basis to said sites in said network.

42. The method claimed in claim 38, wherein said step of providing notification to said sites in said network using said monitoring unit further comprises the step of:

automatically adjusting said form of communication automatically adjusts based on user preference.

43. The method claimed in claim 42, wherein said instructions for adjustment are predefined in a database associated with said monitoring unit.

44. The method claimed in claim 31, further comprising the step of:

backing up said surveillance data in response to said sites detected within a predetermined area.

45. The method claimed in claim 44, wherein said step of backing up said surveillance data in response to said sites detected within a predetermined area further comprises:

backing up said surveillance data in response to detection of signals associated with said sites when said sites enter a predetermined range.

46. The method claimed in claim 31, further comprising the step of:

delaying surveillance for a predetermined period of time.

47. The method claimed in claim 31, further comprising the step of:

automatically deleting surveillance information to create capacity for recording of recent surveillance information.

48. The method claimed in claim 31, further comprising the step of:

automatically adjusting communications with said plurality of sites.

49. The method claimed in claim 48, wherein said step of automatically adjusting communications with said plurality of sites further comprises the step of:

establishing and terminating communications with sites.

AMENDED CLAIMS

[received by the International Bureau on 15 May 2001 (15.05.01); original claims 1-49 replaced by new claims 1-7 (3 pages)]

1. A system for conducting surveillance at a plurality of sites in a network, the system comprising:

a plurality of monitoring units for transmitting and receiving data from and to said plurality of sites;

a communication device for connecting said plurality of sites and said plurality of monitoring units; and

a processor for managing notification of site activity to said plurality of monitoring units, said notification being selectable between broadcast notification in which all the monitoring units are notified simultaneously, sequential notification in which the monitoring units are notified sequentially, and once only notification in which each of the monitoring units are notified once of site activity.

2. The system according to claim 1 wherein said communication device compresses at least two communication selected from a group consisting of an analog telephone line, a cellular line, and ISDN line, a T-1 line, and T-3 line, TCP/IP line, and XDSL line and a frame relay circuits.

3. The system according to claim 1 wherein said processor enables a user to adjust, establish and terminate communication between sites and monitoring units in order to provide selected site touring.

4. A system for conducting surveillance at a plurality of mobile sites, the system comprising:

a monitoring unit, disposed on each of said plurality of mobile sites, for collecting surveillance data on each of said plurality of mobile sites;

a wireless antenna, disposed on each of said plurality of mobile sites, for transmission of surveillance data from each of said plurality of mobile sites;

a wireless receiver, having range of detection, for receiving the transmission of surveillance data from each of said plurality of mobile sites;

a wireless receiver, having a range of detection, for receiving the transmitted surveillance data; and

a backup unit for recording surveillance data from each of said mobile sites when said mobile site is within said range of detection of said wireless receiver.

5. A system for conducting surveillance at a plurality of sites in a network, the system comprising;

a plurality of monitoring units for transmitting and receiving data from and to said plurality of sites.

a communication device for connecting said plurality of sites and said plurality of monitoring units, said communication device comprising at least two communications selected from a group consisting of an analog telephone line, a cellular line, and ISDN line, a T-1 line, a T-3 line, a TCP/IP line, an XDSL line and a frame relay circuit; and

a processor from enabling communication between monitoring units connected to sites and one another by said communication device with different communications.

6. A system for conducting surveillance comprising:

a video unit disposed at a site for transmitting surveillance data;

a plurality of monitor units for displaying the surveillance data; and

a processor for receiving the transmitted surveillance data and relaying the data to first of said plurality of monitor units on a real time basis and to a second of said plurality of monitor units on a delayed time basis thus enabling a viewer to confirm security breaches first witnessed on the first monitor units by viewing the second monitor unit.

7. A system for conducting surveillance comprising:

a video unit disposed at a site for transmitting surveillance data;

a plurality of monitor units for displaying the surveillance data; and

a processor for receiving the transmitted surveillance data and relaying the data firstly to one of said plurality of monitor units and secondly to another of said plurality of monitor units, a delay between relay to the one and the another of the monitor units enabling viewer to confirm security breaches first witnessed on the one monitor unit by viewing the other monitor unit.

STATEMENT UNDER ARTICLE 19 (1)

New claim 1 is supported by the original specification under the heading "Notification" starting on page 10. The system for conducting surveillance in accordance with the present invention includes a processor which is selectable between broadcast notification, sequential notification and once only notification. None of the prior art shows the selectablilty.

Claim 2 provides for the communication device for connecting to the plurality of sites and plurality of monitors, as including, at least two communications selected from a group.

Claim 3 provides for the processor to adjust, establish and terminate communication between he sites and the monitoring units over these various communication lines.

Claim 4 more clearly defines the system as a remote backup as described in the original specification under the heading "Remote Backup" beginning on page 14. None of the references found in the search show monitoring units on mobile sites with wireless antennas and receivers for automatically backing up surveillance data from the mobile sites when the mobile sites is within a range of detection of the wireless receiver.

New claim 18 is based on the original disclosure under the heading "Video Pass Thru" beginning on page 18. This claim defines a system for conducting surveillance utilizing a plurality of monitoring units interconnected on various communication lines and a processor for enabling communication between the monitoring units connected to the sites and one another by different communication lines. None of the art provided in the search results shows this configuration.

Claims 6 and 7 define support in the original specification on page 20 under the heading "Video Delay" and in Figure 27. None of the references in the search report provide for a processor for relaying data to a first of a plurality of monitors on a real time basis and to a second of the monitors on a delayed time basis and in order to enable a viewer to confirm security breaches first witnessed on the first monitor by viewing the second monitor.

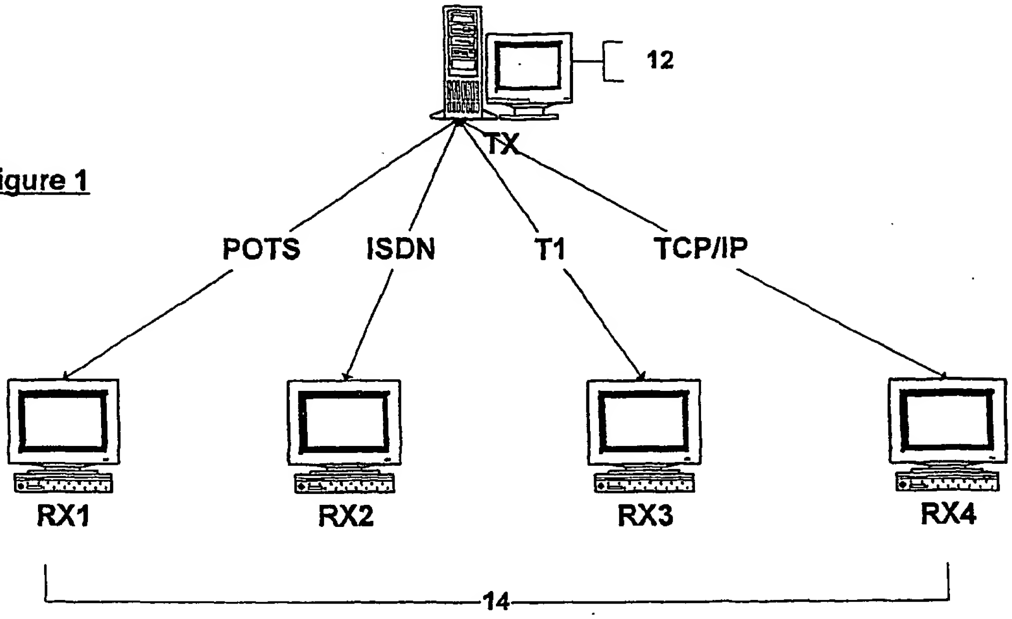


Figure 1

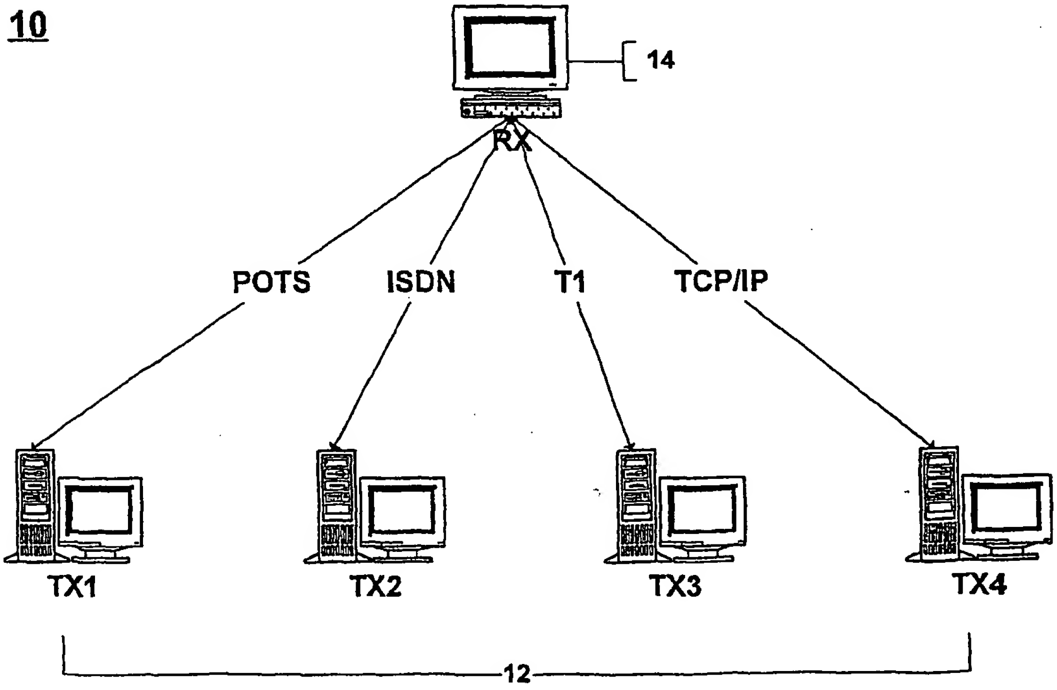


Figure 2

figure 3

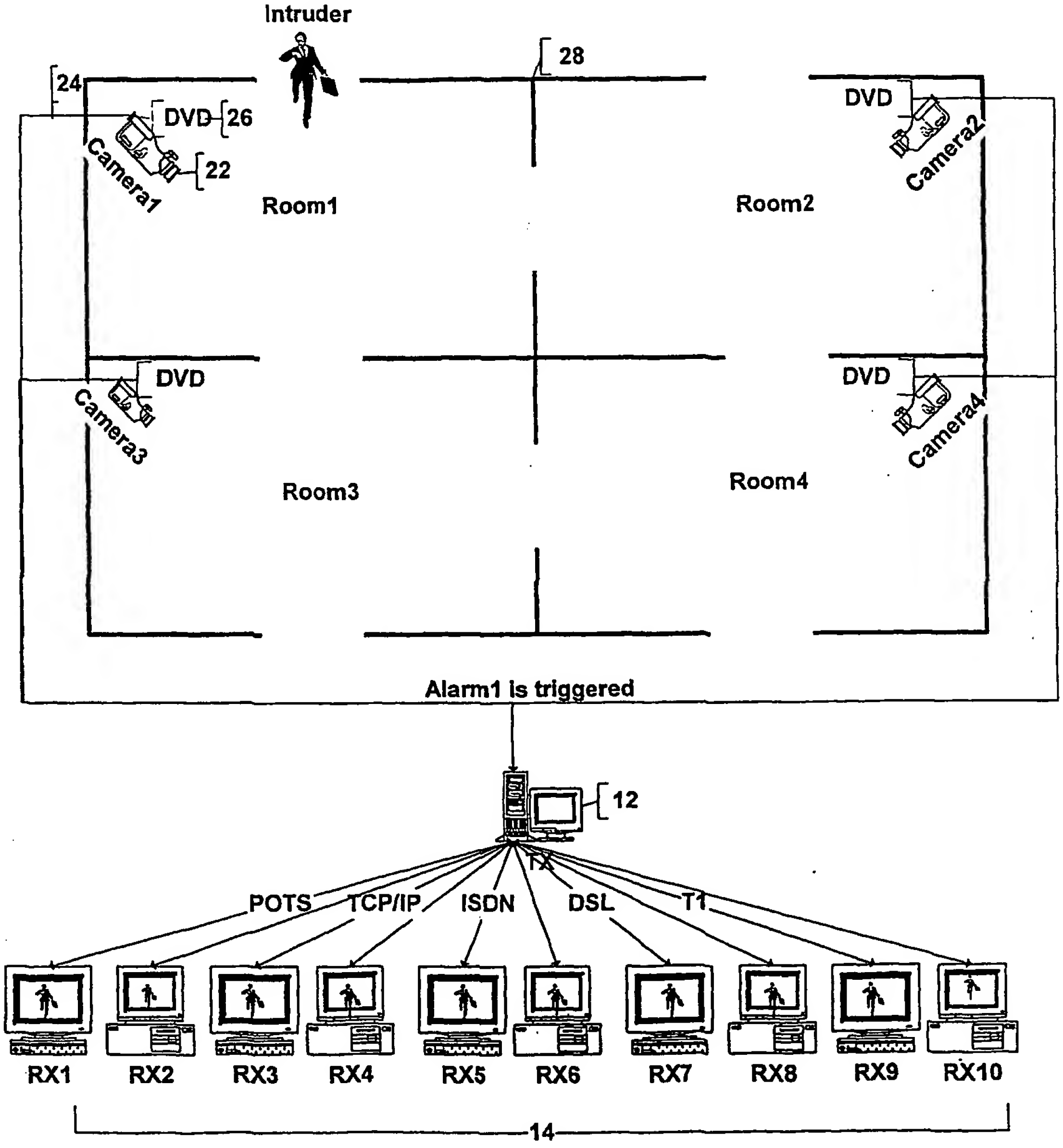

Intruder
28
24
DVD
26
22
Camera1
Room1
DVD
Camera2
Room2
DVD
Camera3
Room3
DVD
Camera4
Room4
Alarm1 is triggered
12
TX
POTS
TCP/IP
ISDN
DSL
T1
RX1
RX2
RX3
RX4
RX5
RX6
RX7
RX8
RX9
RX10
14

Figure 4

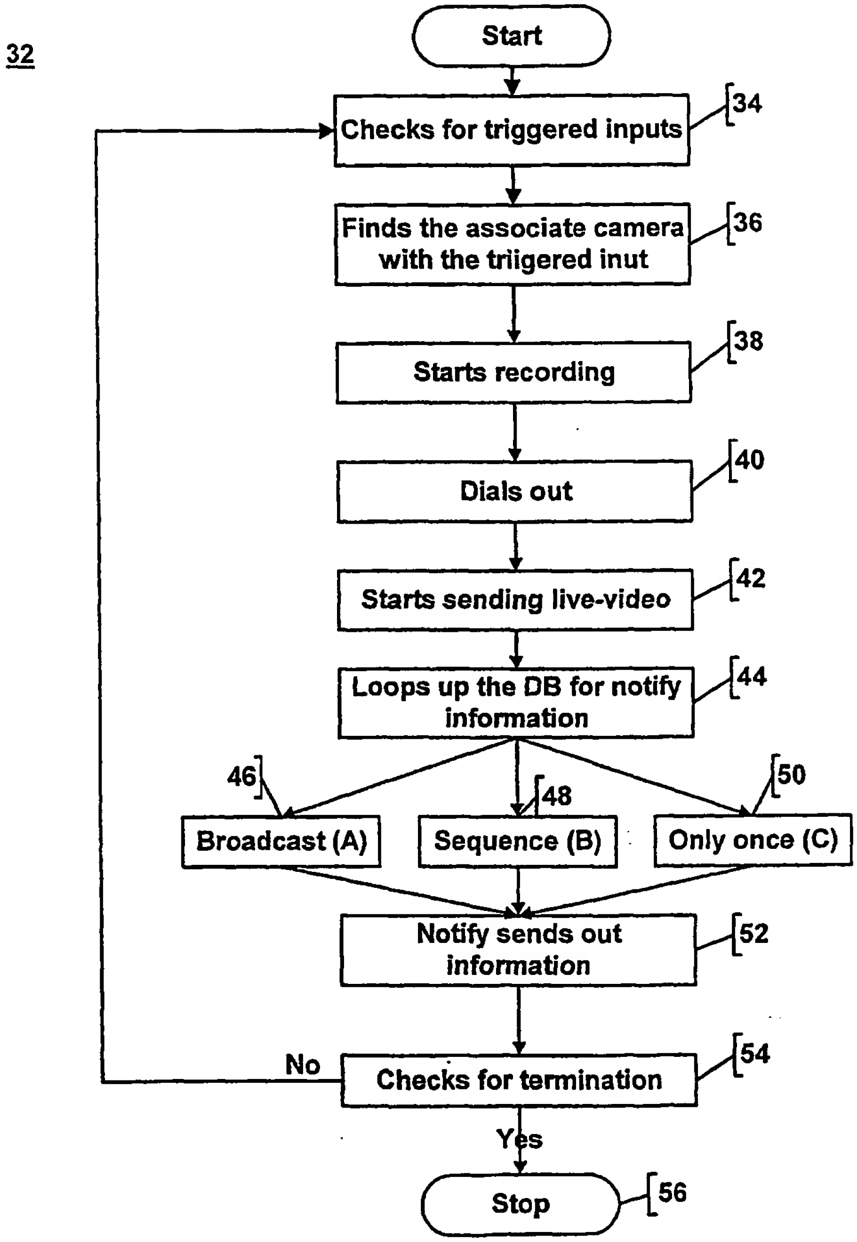

32
Start
Checks for triggered inputs
34
Finds the associate camera with the triigered inut
36
Starts recording
38
Dials out
40
Starts sending live-video
42
Loops up the DB for notify information
44
46
Broadcast (A)
48
Sequence (B)
50
Only once (C)
Notify sends out information
52
No
Checks for termination
54
Yes
Stop
56

figure 5

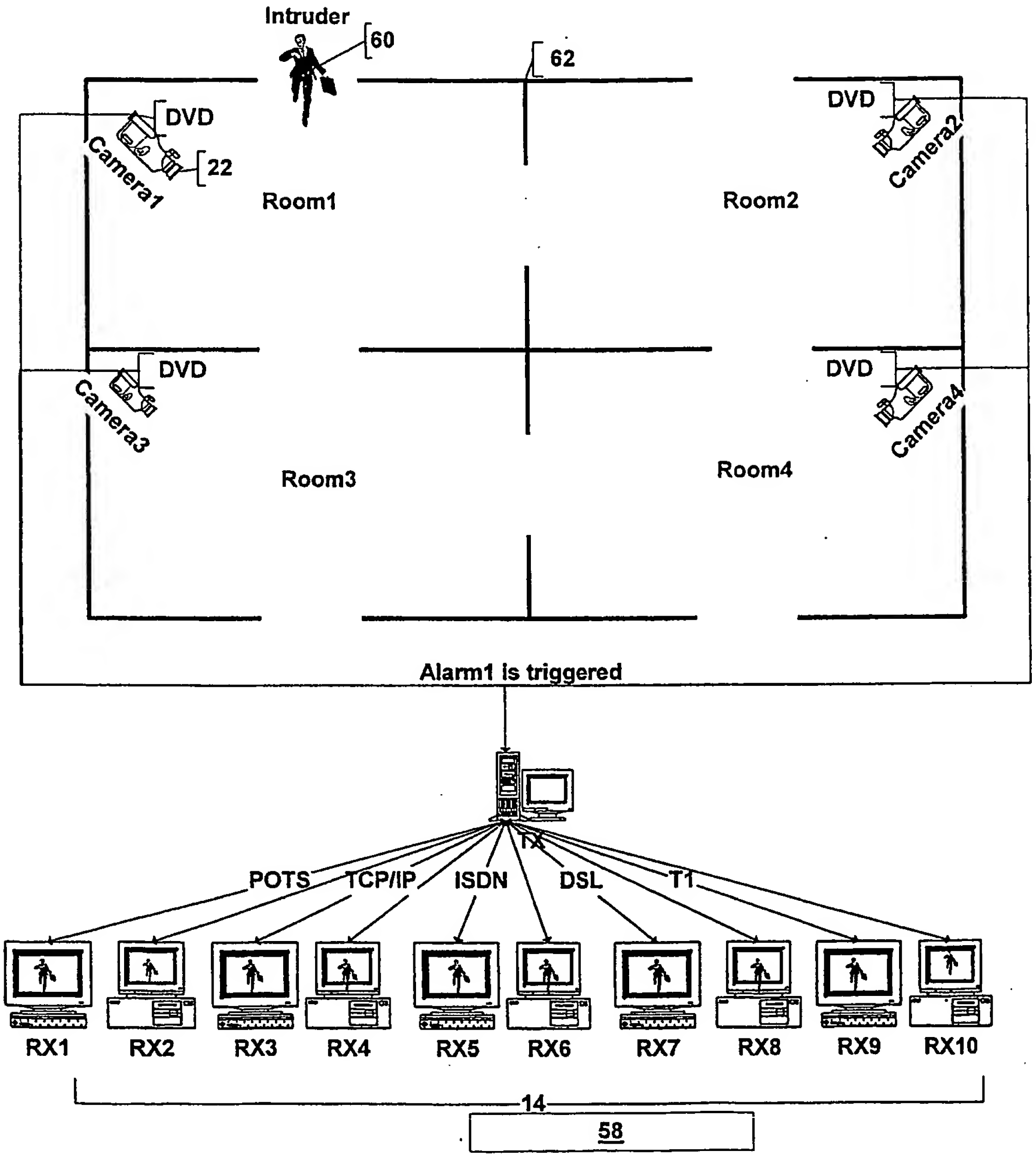

Intruder
60
62
DVD
Camera1
22
Room1
DVD
Camera2
Room2
DVD
Camera3
Room3
DVD
Camera4
Room4
Alarm1 is triggered
TX
POTS
TCP/IP
ISDN
DSL
T1
RX1
RX2
RX3
RX4
RX5
RX6
RX7
RX8
RX9
RX10
14
58

Figure 6

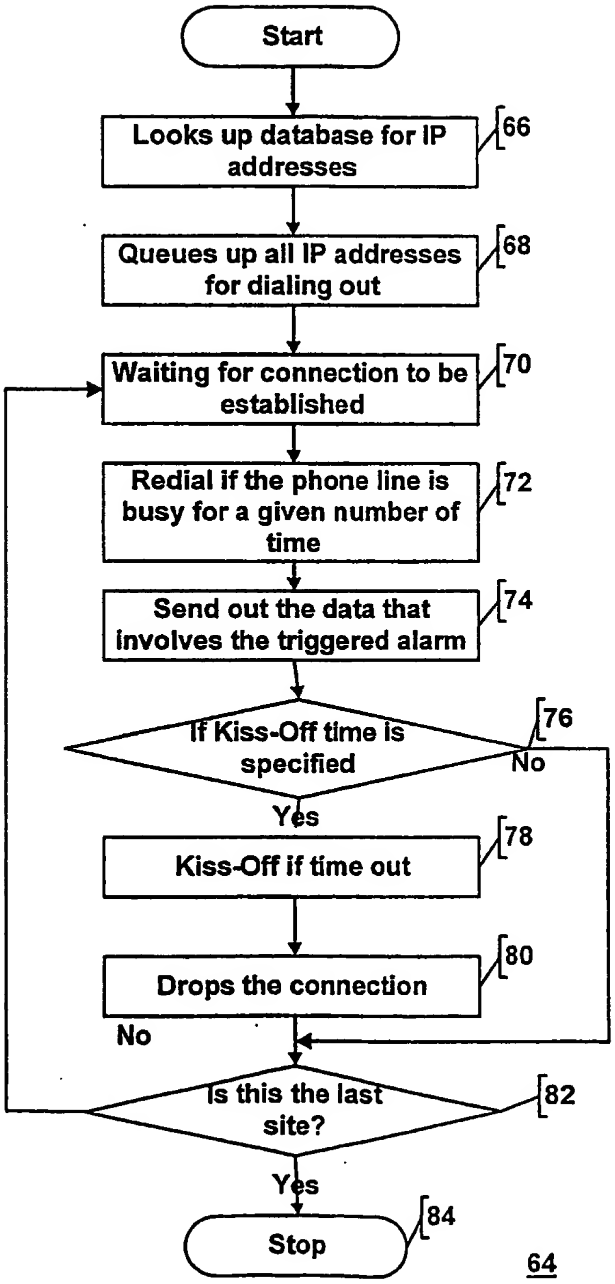
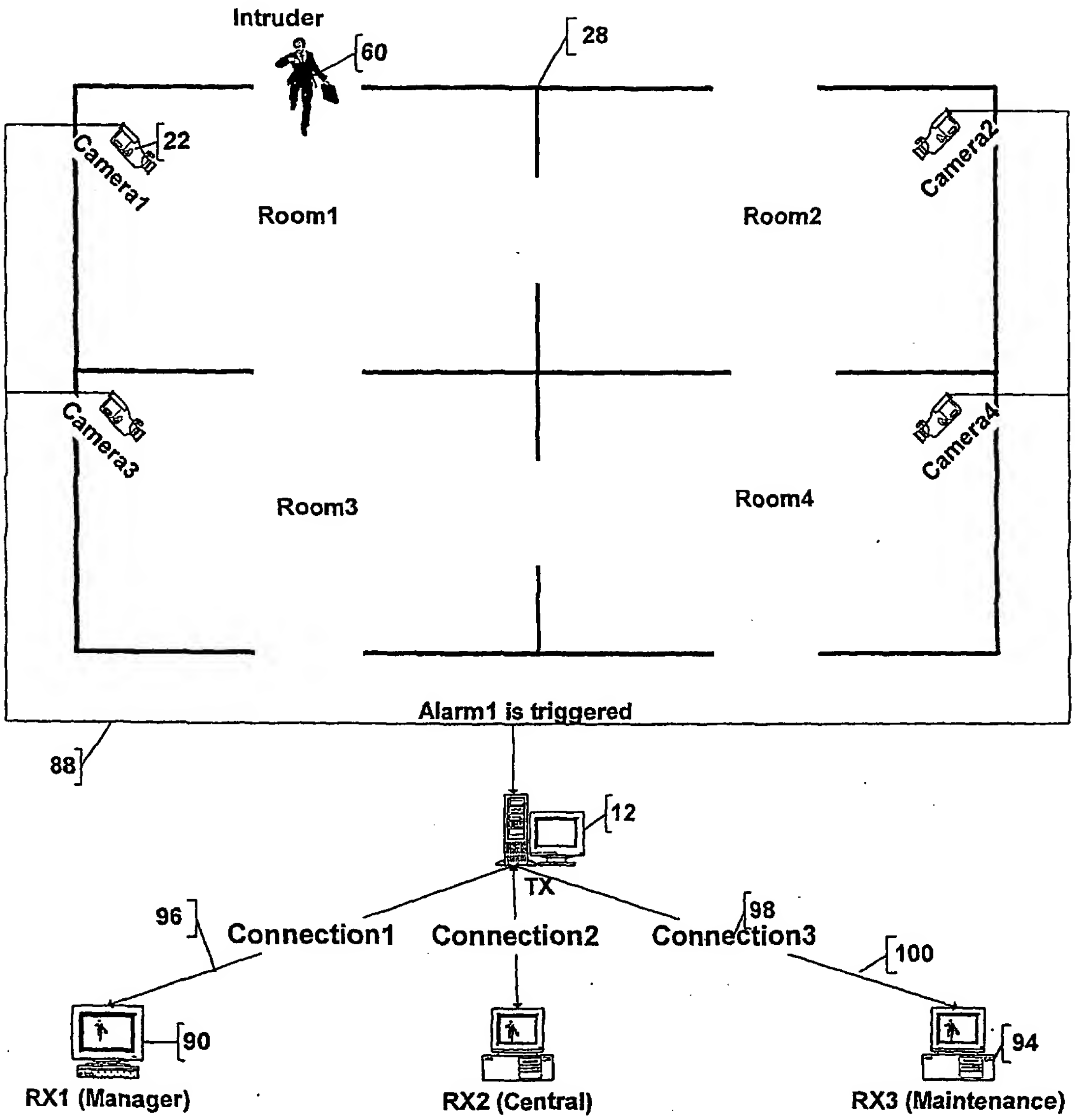
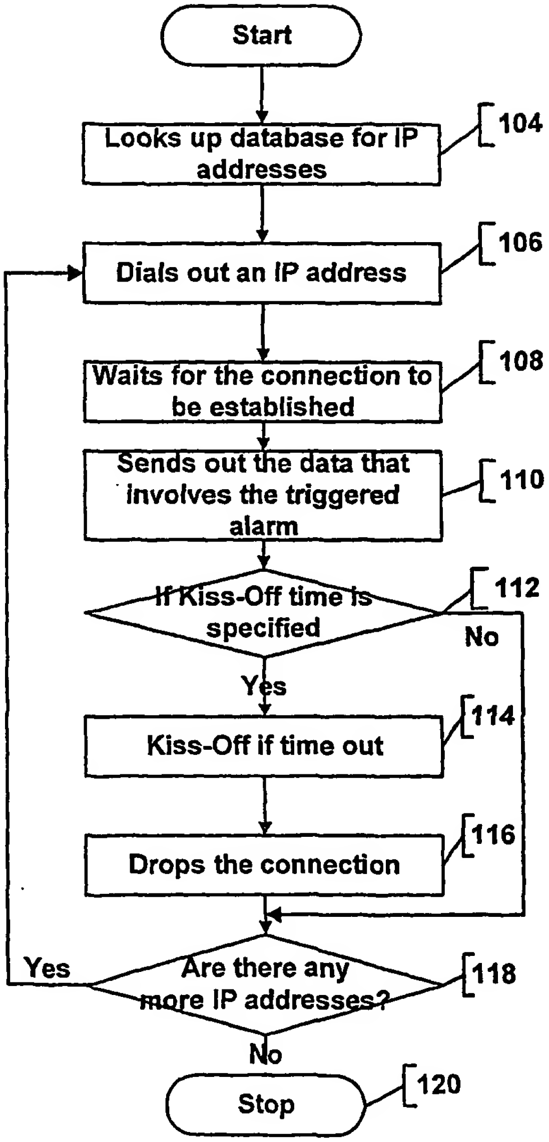

Start
Looks up database for IP addresses
66
Queues up all IP addresses for dialing out
68
Waiting for connection to be established
70
Redial if the phone line is busy for a given number of time
72
Send out the data that involves the triggered alarm
74
If Kiss-Off time is specified
76
No
Yes
Kiss-Off if time out
78
Drops the connection
80
No
Is this the last site?
82
Yes
Stop
84
64

Figure 7


Intruder
60
28
22
Camera1
Camera2
Room1
Room2
Camera3
Camera4
Room3
Room4
Alarm1 is triggered
88
12
TX
96
Connection1
Connection2
98
Connection3
100
90
94
RX1 (Manager)
RX2 (Central)
RX3 (Maintenance)

86

Figure 8


Start
Looks up database for IP addresses
104
Dials out an IP address
106
Waits for the connection to be established
108
Sends out the data that involves the triggered alarm
110
If Kiss-Off time is specified
112
No
Yes
Kiss-Off if time out
114
Drops the connection
116
Yes
Are there any more IP addresses?
118
No
Stop
120

102

Figure 9

122

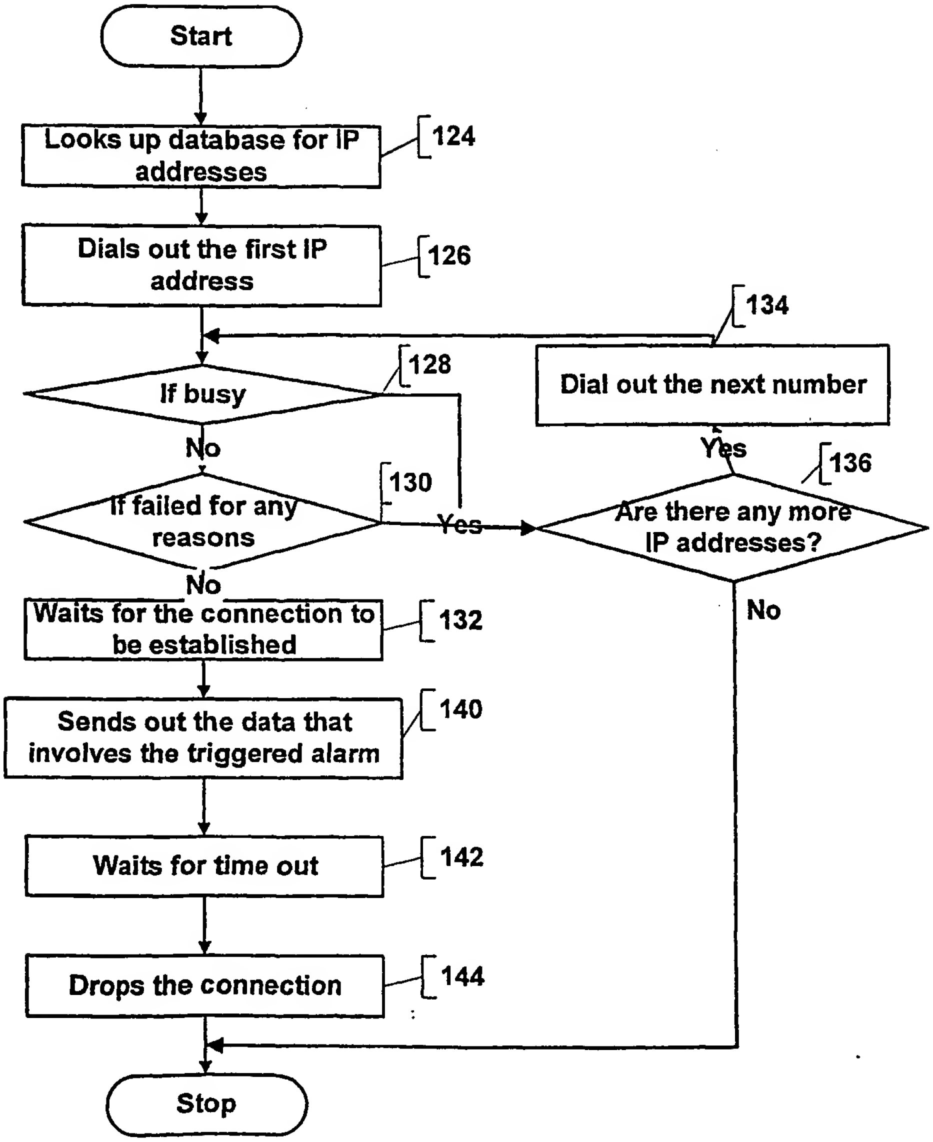

Start
Looks up database for IP addresses
124
Dials out the first IP address
126
134
Dial out the next number
If busy
128
No
Yes
136
130
If failed for any reasons
Yes
Are there any more IP addresses?
No
No
Waits for the connection to be established
132
Sends out the data that involves the triggered alarm
140
Waits for time out
142
Drops the connection
144
Stop

Figure 10

118

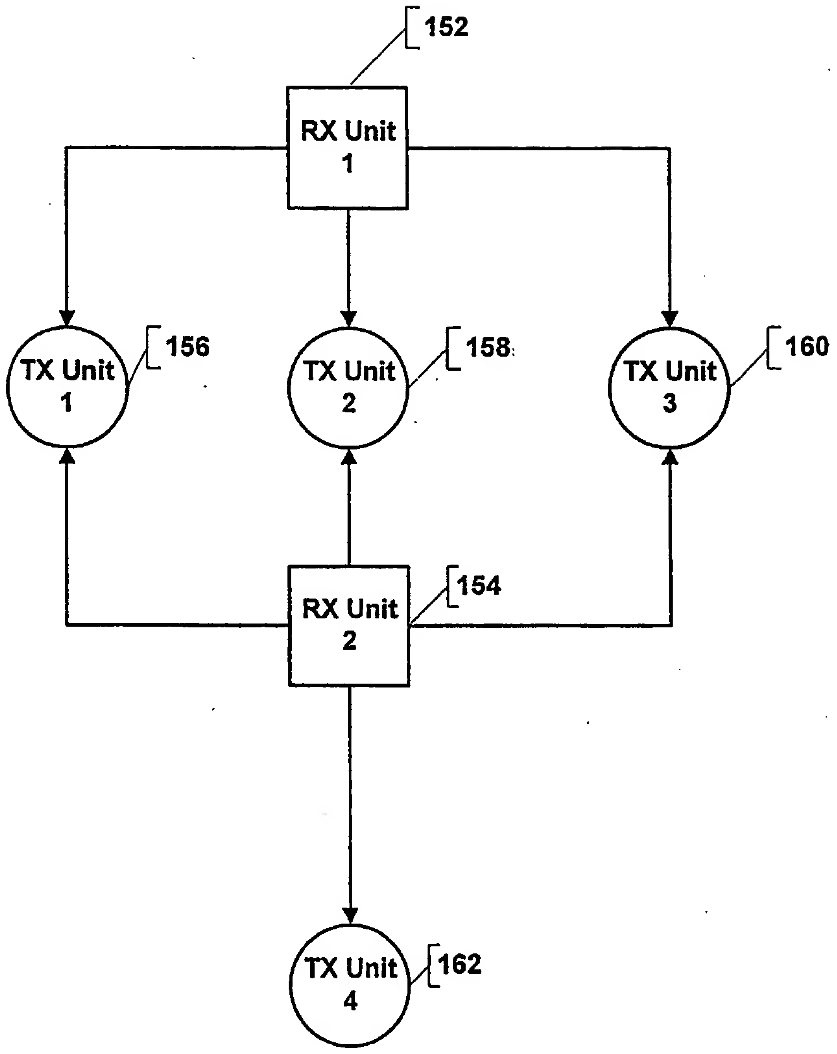


Figure 11

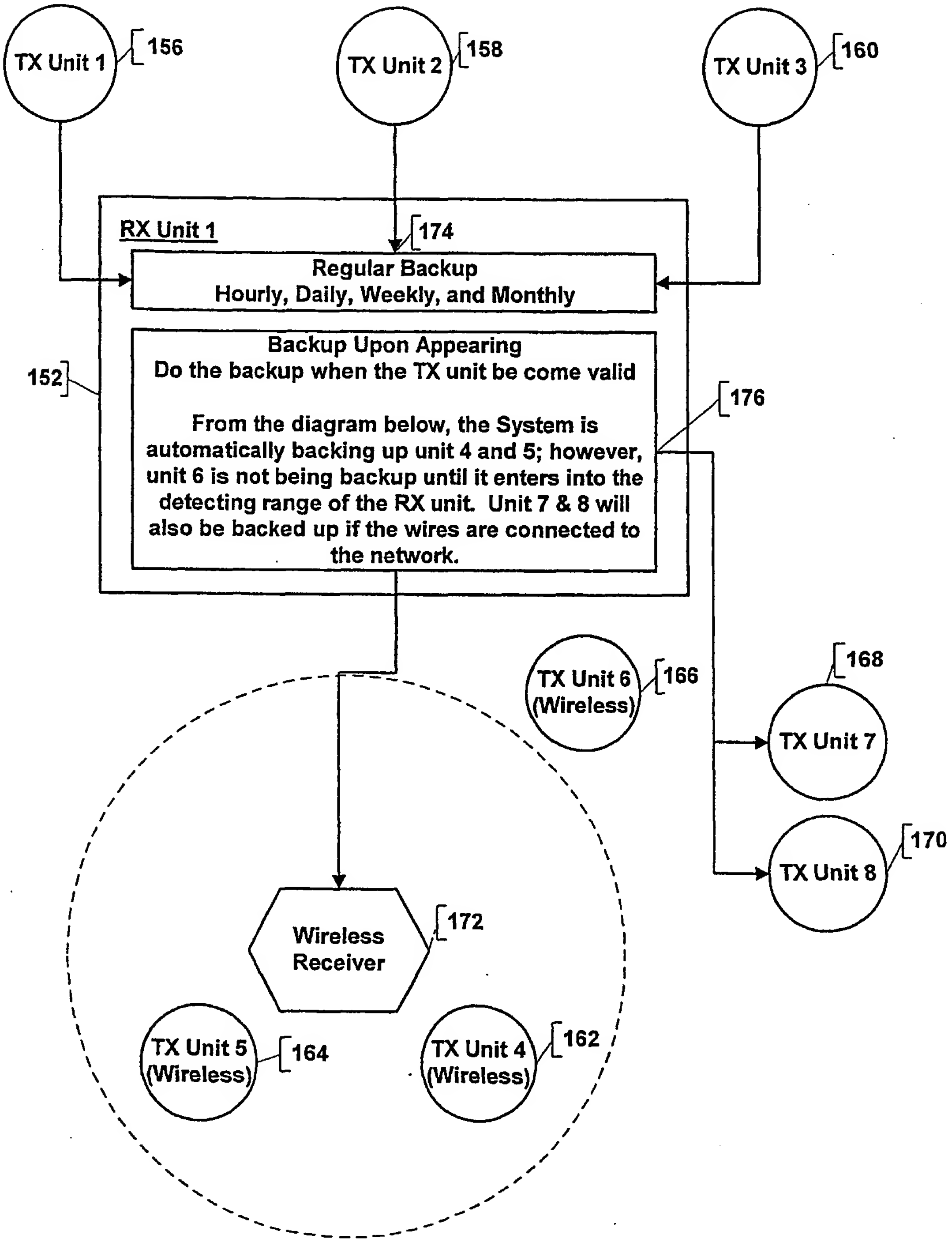

TX Unit 1
156
TX Unit 2
158
TX Unit 3
160
RX Unit 1
174
Regular Backup
Hourly, Daily, Weekly, and Monthly
Backup Upon Appearing
Do the backup when the TX unit be come valid
From the diagram below, the System is automatically backing up unit 4 and 5; however, unit 6 is not being backup until it enters into the detecting range of the RX unit. Unit 7 & 8 will also be backed up if the wires are connected to the network.
152
176
TX Unit 6 (Wireless)
166
168
TX Unit 7
TX Unit 8
170
Wireless Receiver
172
TX Unit 5 (Wireless)
164
TX Unit 4 (Wireless)
162

Figure 12

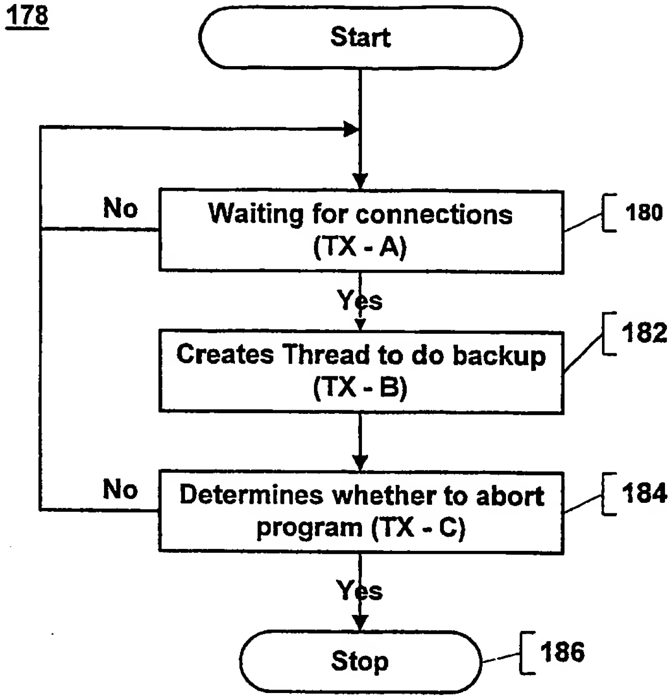

178
Start
Waiting for connections (TX - A)
180
No
Yes
Creates Thread to do backup (TX - B)
182
Determines whether to abort program (TX - C)
184
No
Yes
Stop
186

Figure 13

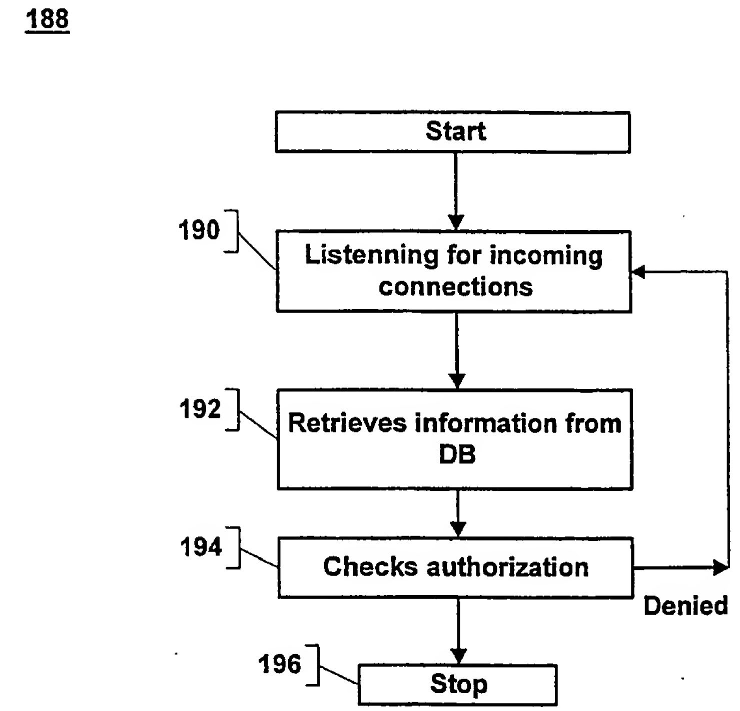

188
Start
190
Listenning for incoming connections
192
Retrieves information from DB
194
Checks authorization
Denied
196
Stop

Figure 14

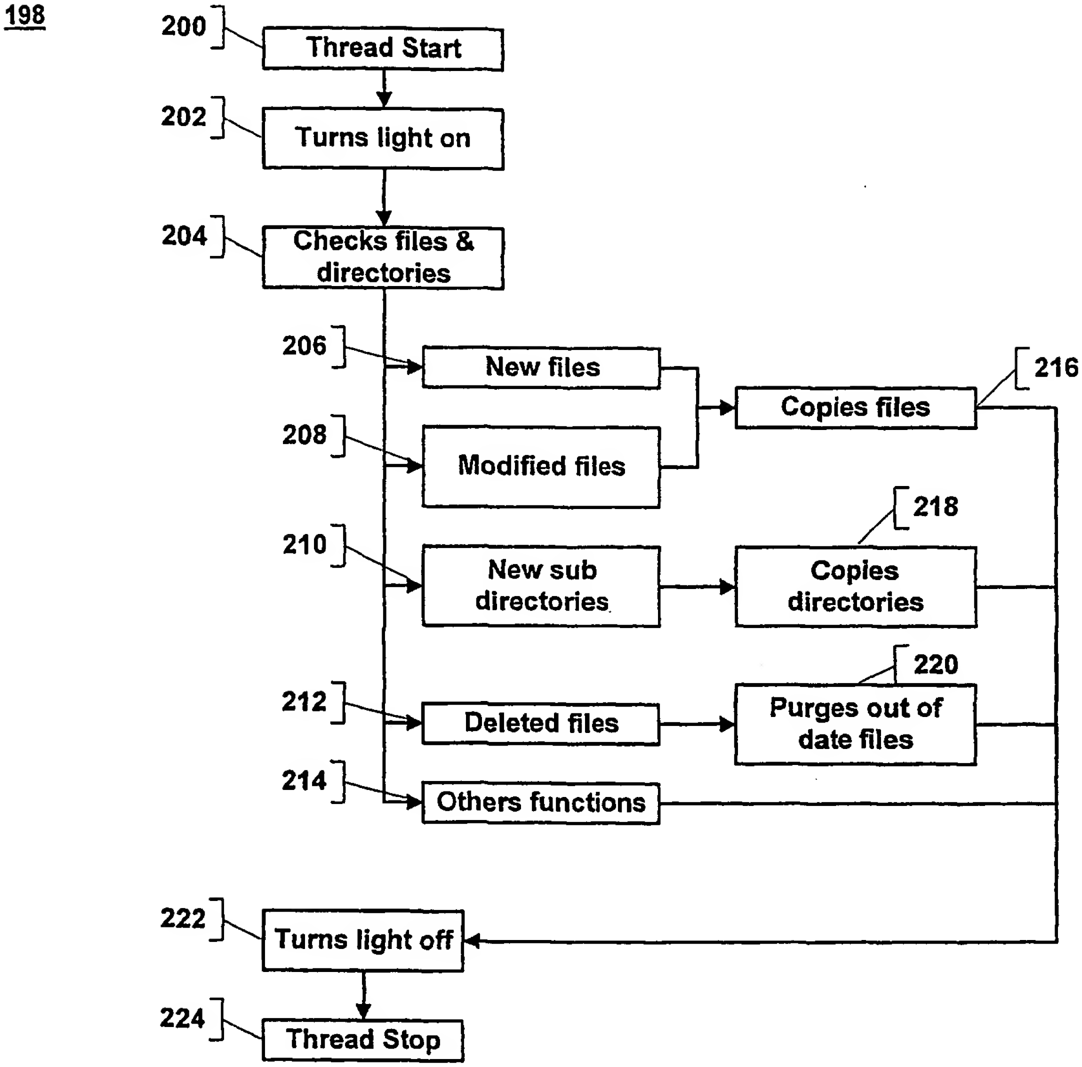

198
200
Thread Start
202
Turns light on
204
Checks files & directories
206
New files
208
Modified files
210
New sub directories
212
Deleted files
214
Others functions
216
Copies files
218
Copies directories
220
Purges out of date files
222
Turns light off
224
Thread Stop

Figure 15

226

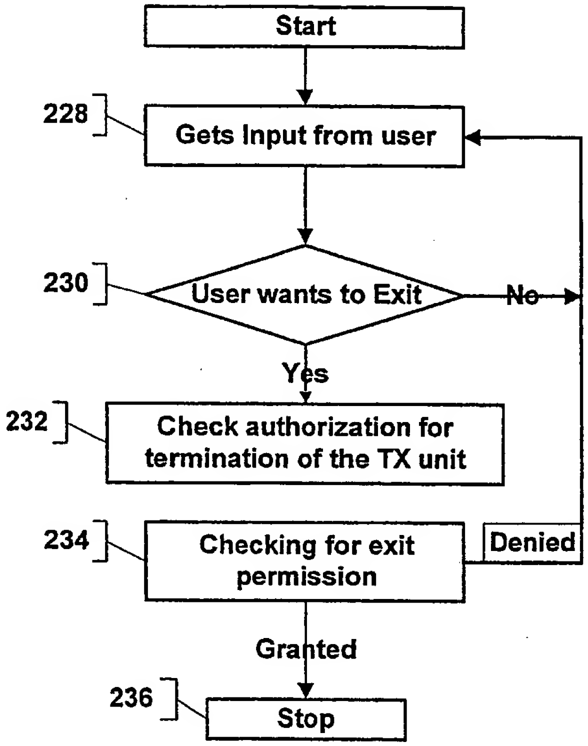


Figure 16

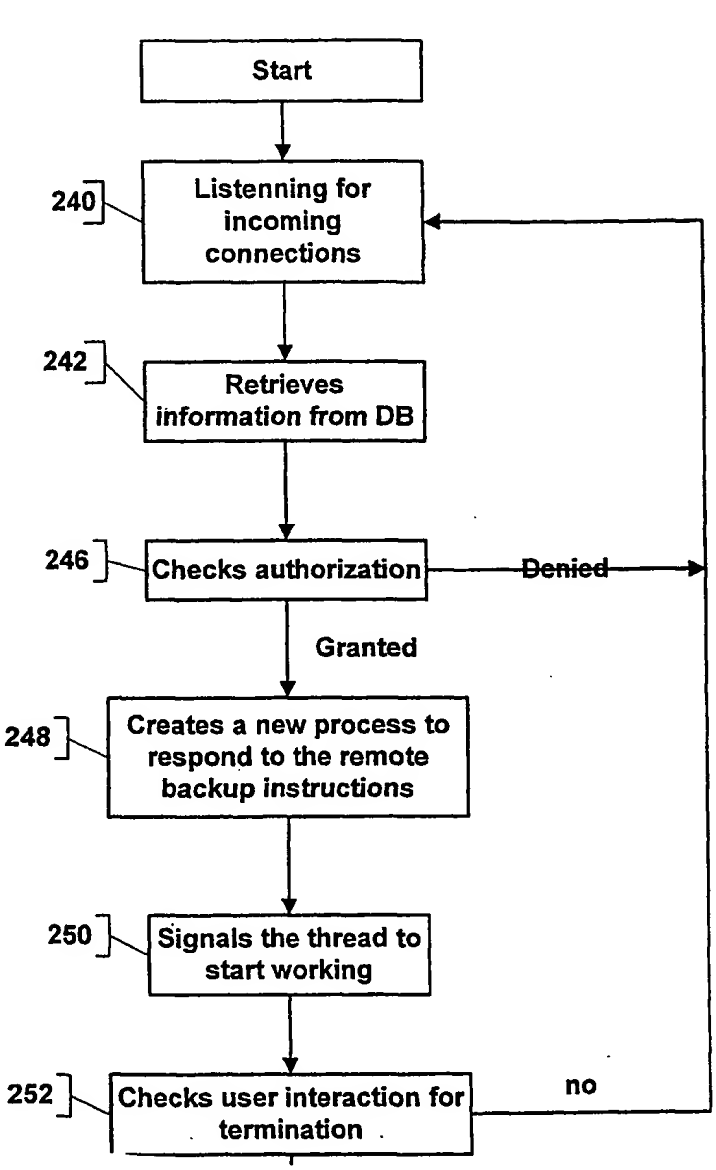

238
Start
240
Listenning for incoming connections
242
Retrieves information from DB
246
Checks authorization
~~Denied~~
Granted
248
Creates a new process to respond to the remote backup instructions
250
Signals the thread to start working
252
Checks user interaction for termination
no

Figure 17

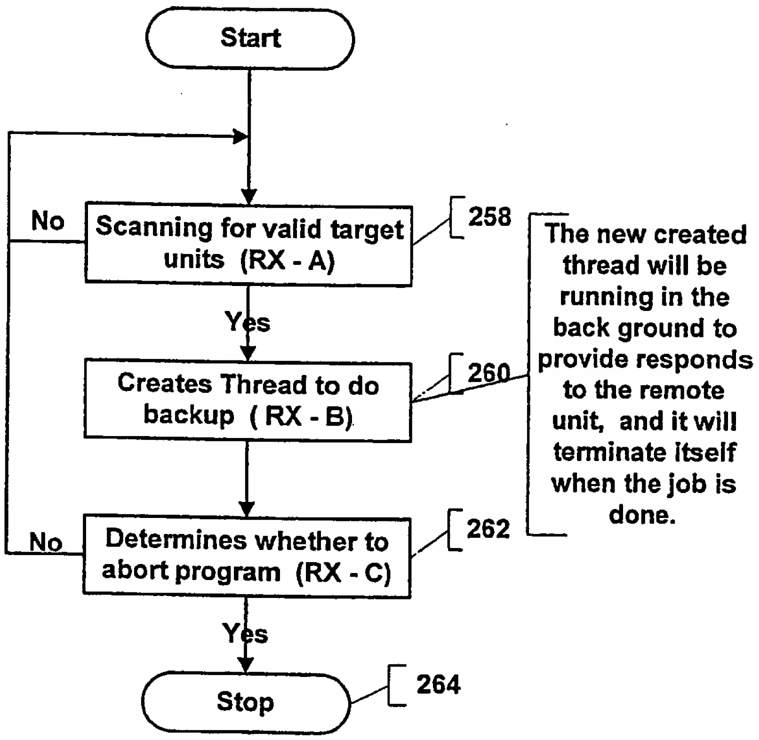

256
Start
No
Scanning for valid target units (RX - A)
258
Yes
Creates Thread to do backup (RX - B)
260
The new created thread will be running in the back ground to provide responds to the remote unit, and it will terminate itself when the job is done.
No
Determines whether to abort program (RX - C)
262
Yes
Stop
264

Figure 18

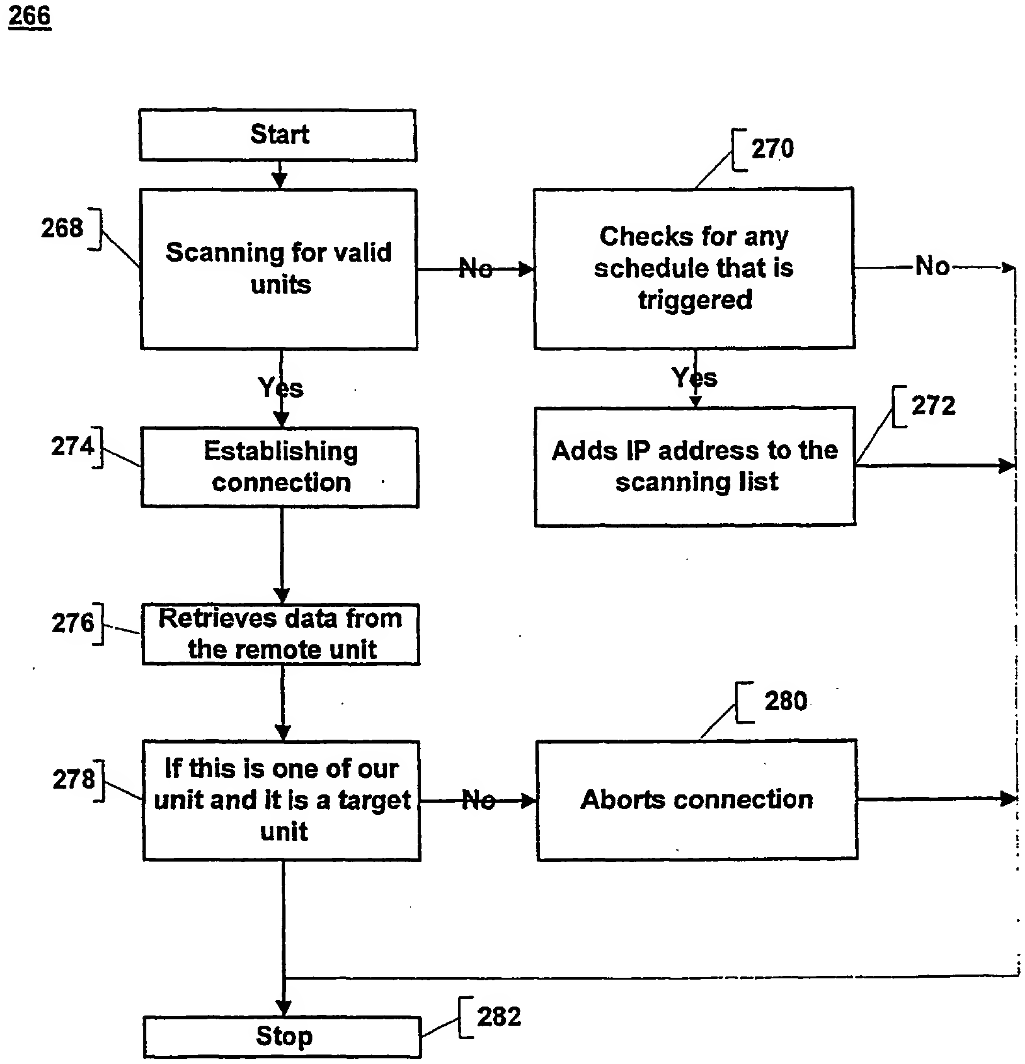

266
Start
268
Scanning for valid units
No
270
Checks for any schedule that is triggered
No
Yes
Yes
274
Establishing connection
272
Adds IP address to the scanning list
276
Retrieves data from the remote unit
280
278
If this is one of our unit and it is a target unit
No
Aborts connection
Stop
282

Figure 19

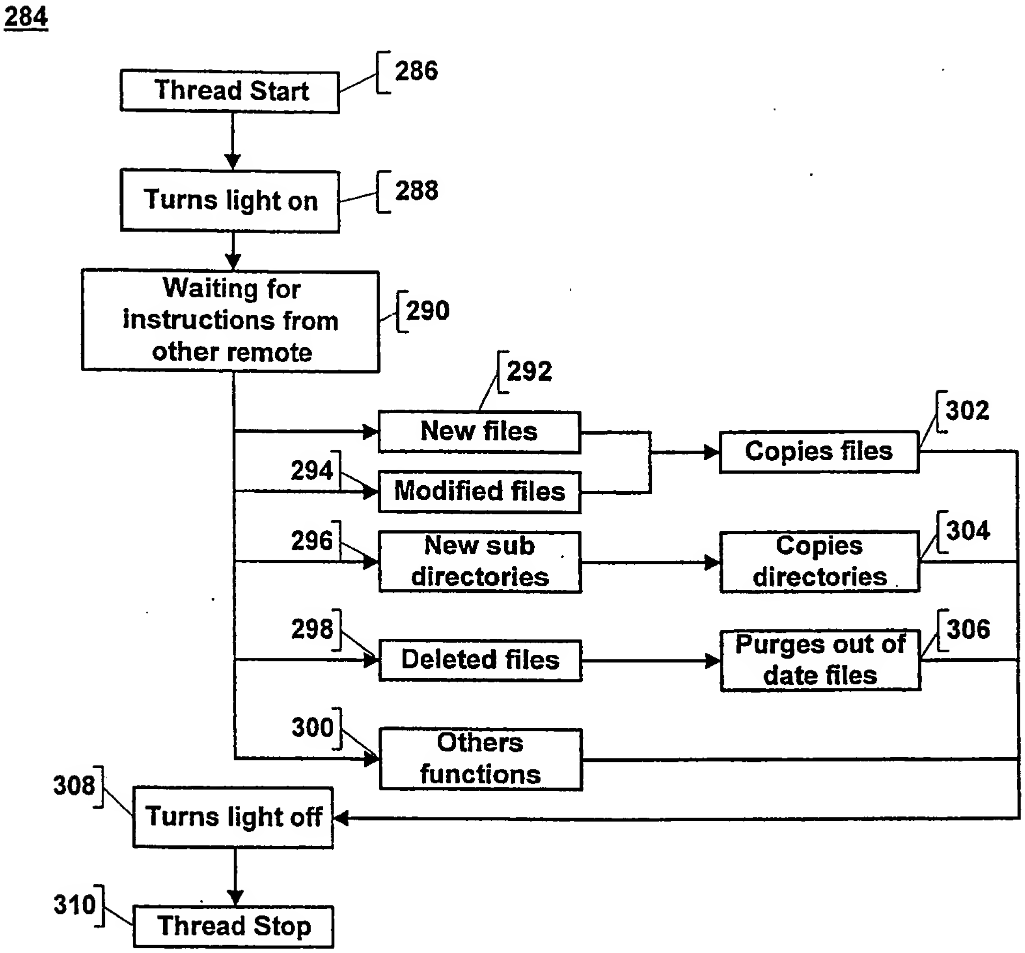

284
Thread Start
286
Turns light on
288
Waiting for instructions from other remote
290
292
New files
294
Modified files
Copies files
302
296
New sub directories
Copies directories
304
298
Deleted files
Purges out of date files
306
300
Others functions
308
Turns light off
310
Thread Stop

Figure 20

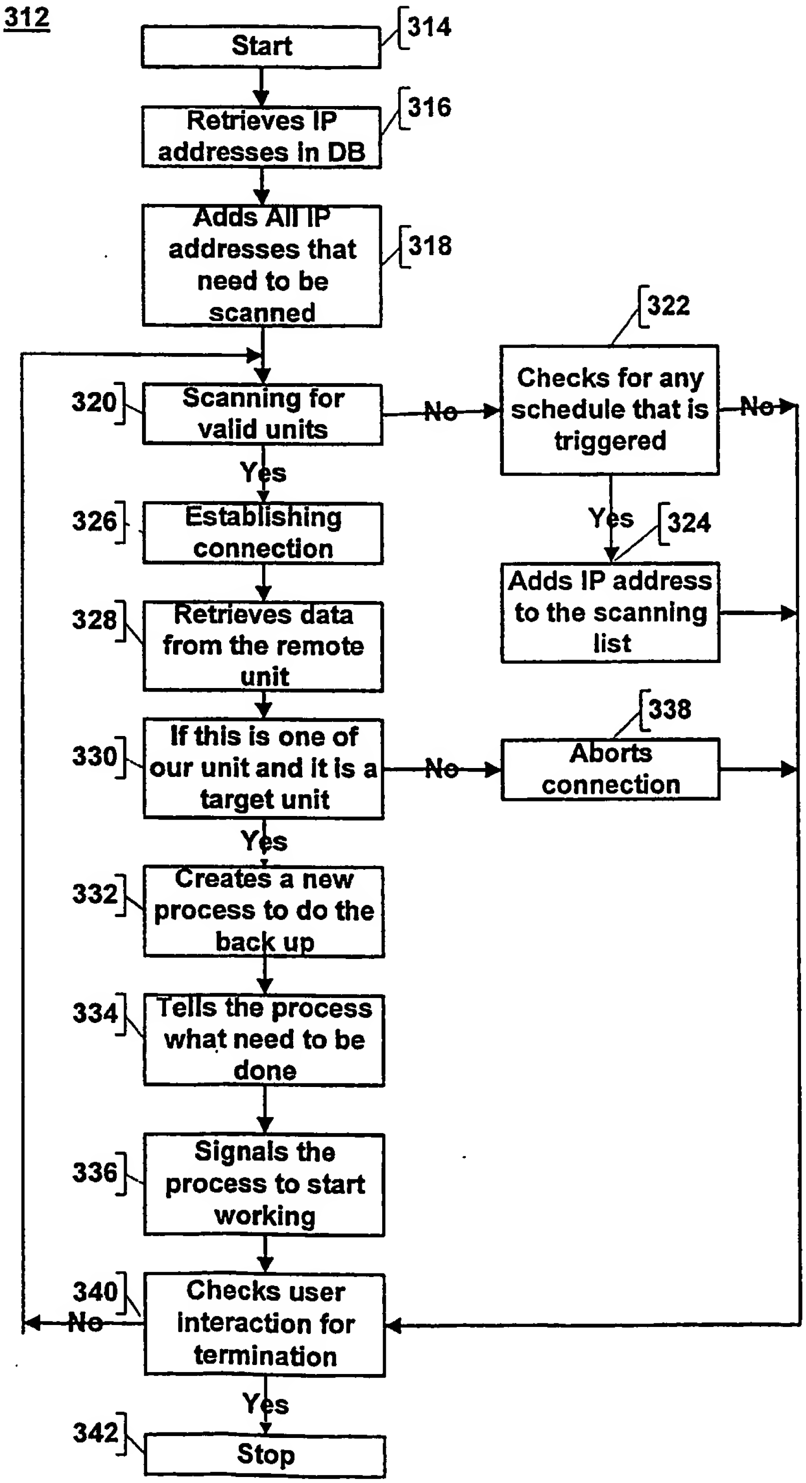

312
Start
314
Retrieves IP addresses in DB
316
Adds All IP addresses that need to be scanned
318
322
Scanning for valid units
320
No
Checks for any schedule that is triggered
No
Yes
Yes
324
Establishing connection
326
Adds IP address to the scanning list
Retrieves data from the remote unit
328
338
If this is one of our unit and it is a target unit
330
No
Aborts connection
Yes
Creates a new process to do the back up
332
Tells the process what need to be done
334
Signals the process to start working
336
Checks user interaction for termination
340
No
Yes
Stop
342

Figure 21

346

From the diagram above, the TX1 can not connect to the TX2 due to the different type of connections. However, data of the TX1 may be send to the TX2 by using the RX as a message pass-on station. Therefore, the message will be sent from the TX1 to the RX. When the RX receives the message, it will send the message to the TX2.

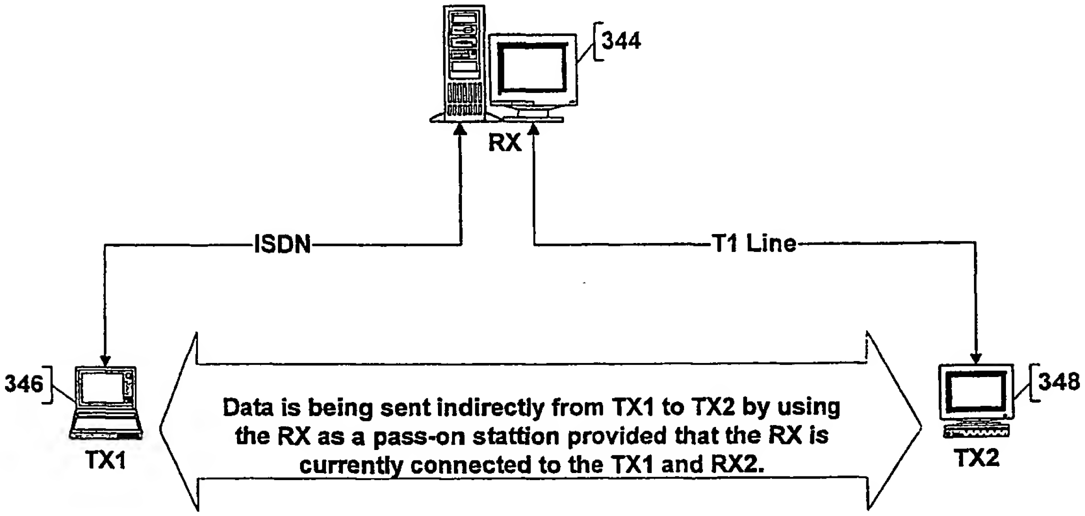

344
RX
ISDN
T1 Line
346
TX1
348
TX2
Data is being sent indirectly from TX1 to TX2 by using the RX as a pass-on stattion provided that the RX is currently connected to the TX1 and RX2.

Figure 22

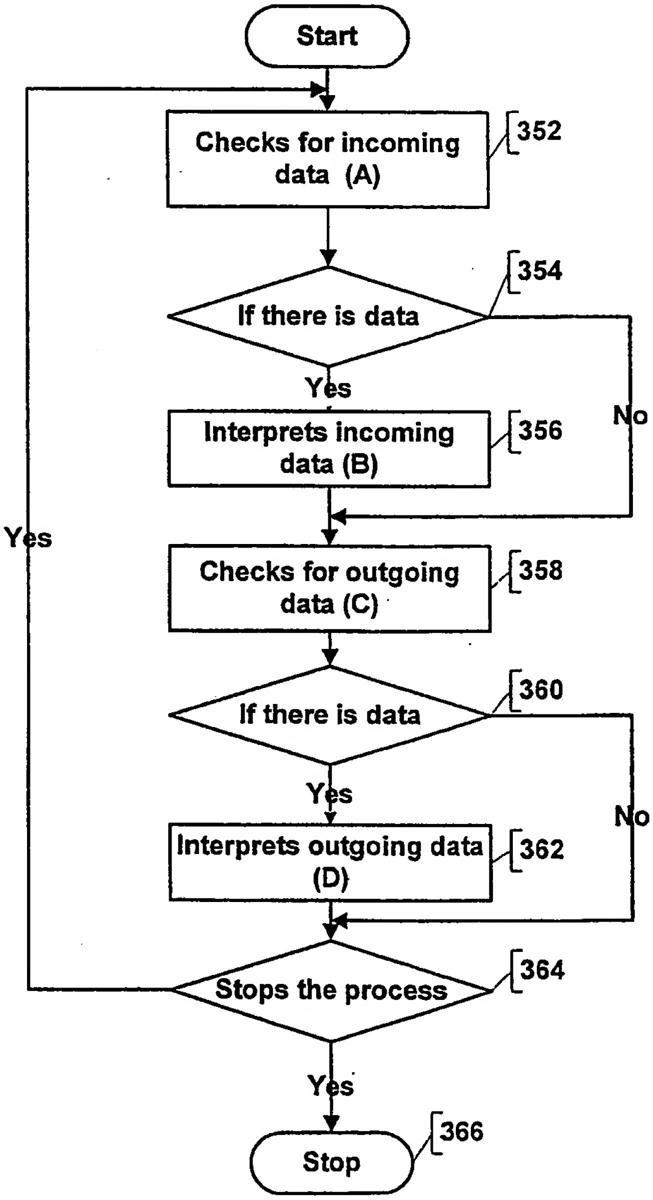

350
Start
Checks for incoming data (A)
352
If there is data
354
Yes
No
Interprets incoming data (B)
356
Checks for outgoing data (C)
358
If there is data
360
Yes
No
Interprets outgoing data (D)
362
Stops the process
364
Yes
Yes
Stop
366

Figure 23

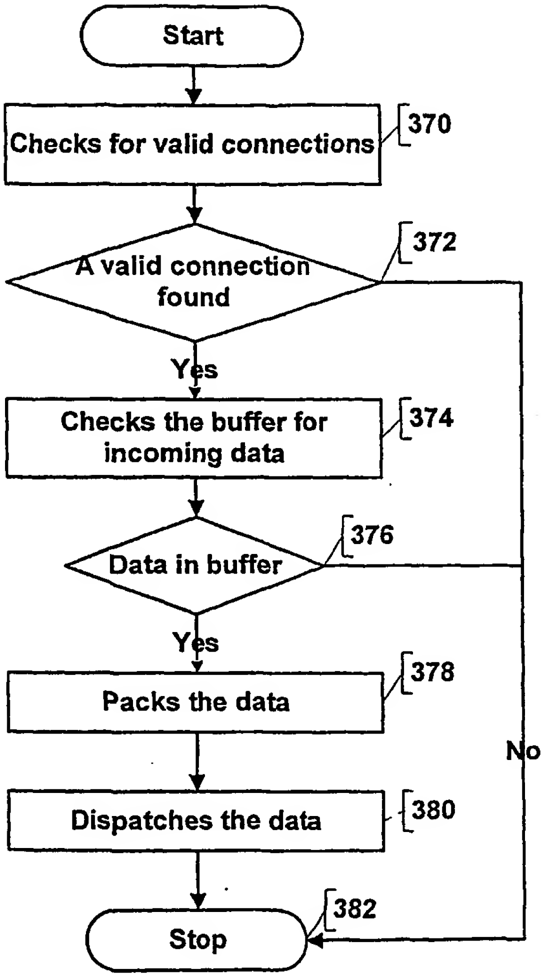

Start
Checks for valid connections
370
A valid connection found
372
Yes
Checks the buffer for incoming data
374
Data in buffer
376
Yes
Packs the data
378
No
Dispatches the data
380
Stop
382

Figure 24

384

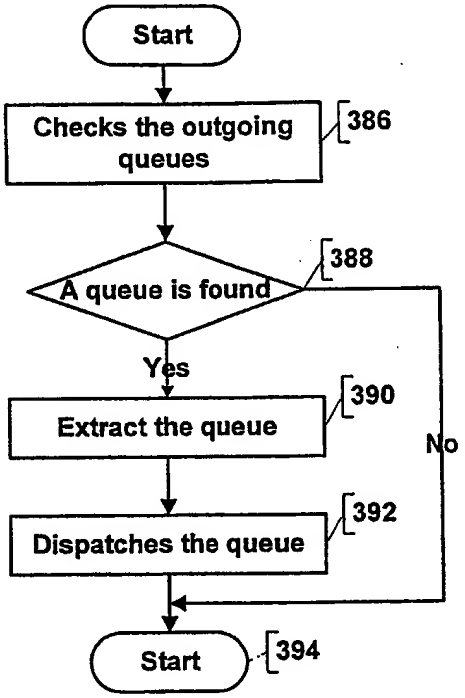


Figure 25

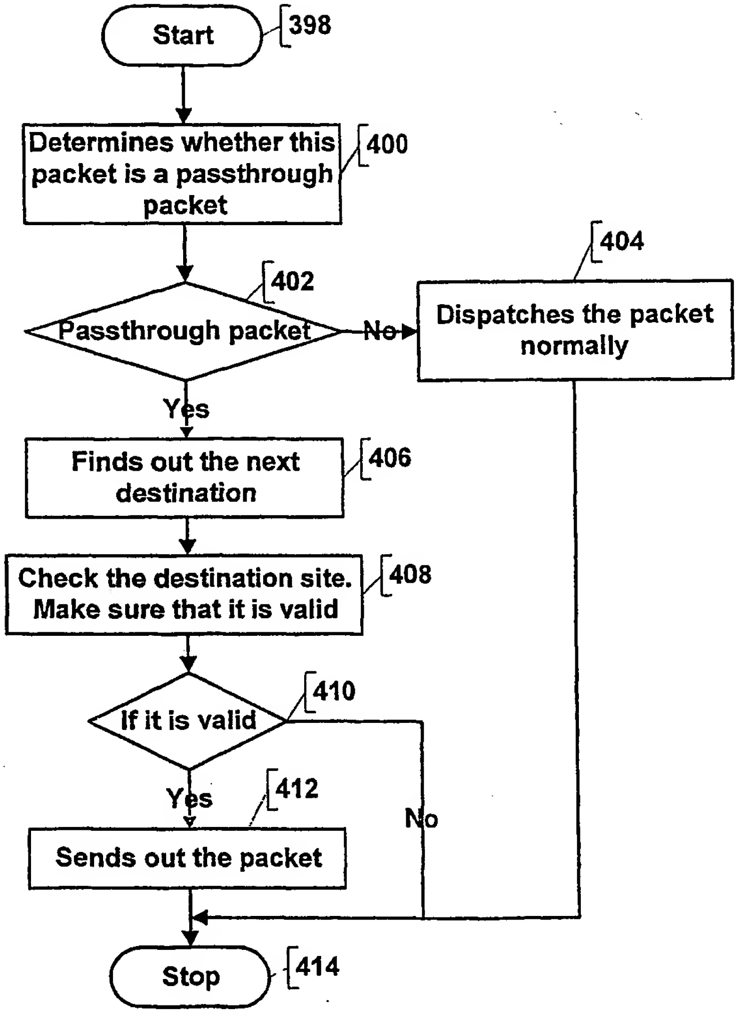

396
Start
398
Determines whether this packet is a passthrough packet
400
Passthrough packet
402
No
Dispatches the packet normally
404
Yes
Finds out the next destination
406
Check the destination site. Make sure that it is valid
408
If it is valid
410
Yes
412
No
Sends out the packet
Stop
414

Figure 26

416

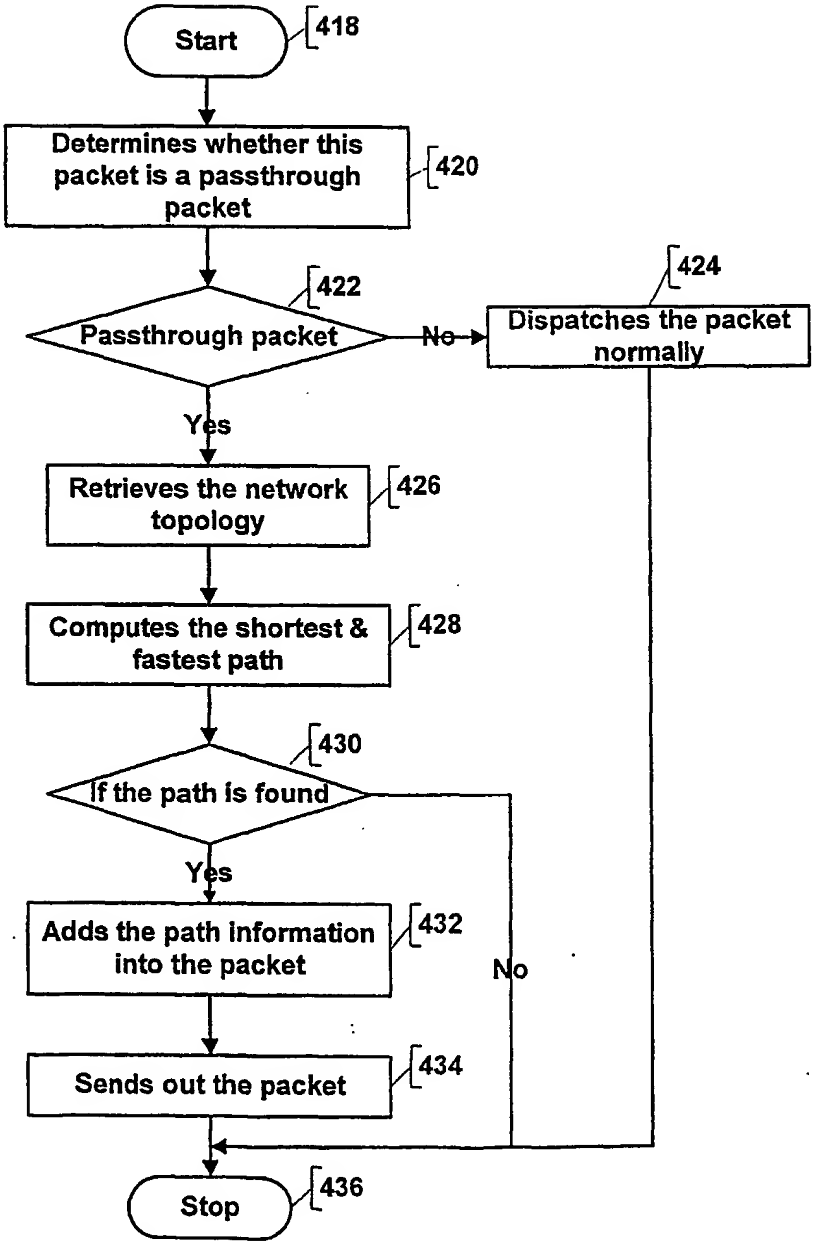

Start
418
Determines whether this packet is a passthrough packet
420
422
Passthrough packet
No
424
Dispatches the packet normally
Yes
Retrieves the network topology
426
Computes the shortest & fastest path
428
430
If the path is found
Yes
Adds the path information into the packet
432
No
Sends out the packet
434
Stop
436

Figure 27

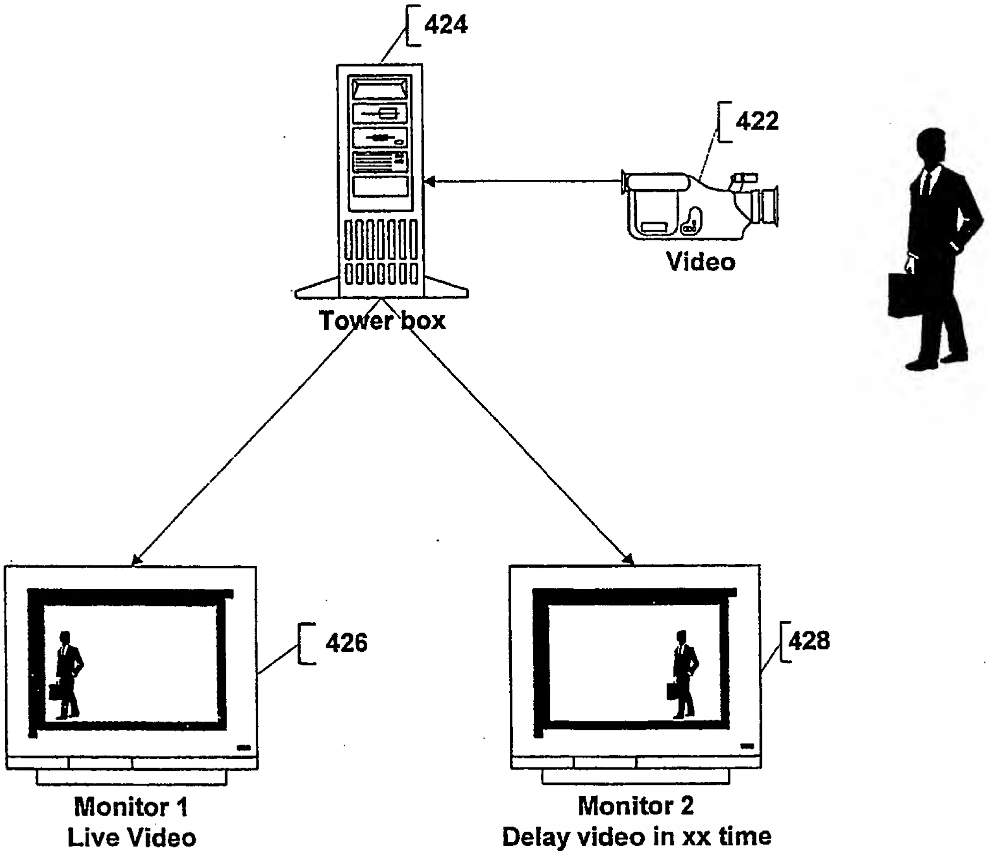

424
422
Video
Tower box
426
428
Monitor 1
Live Video
Monitor 2
Delay video in xx time

Figure 28

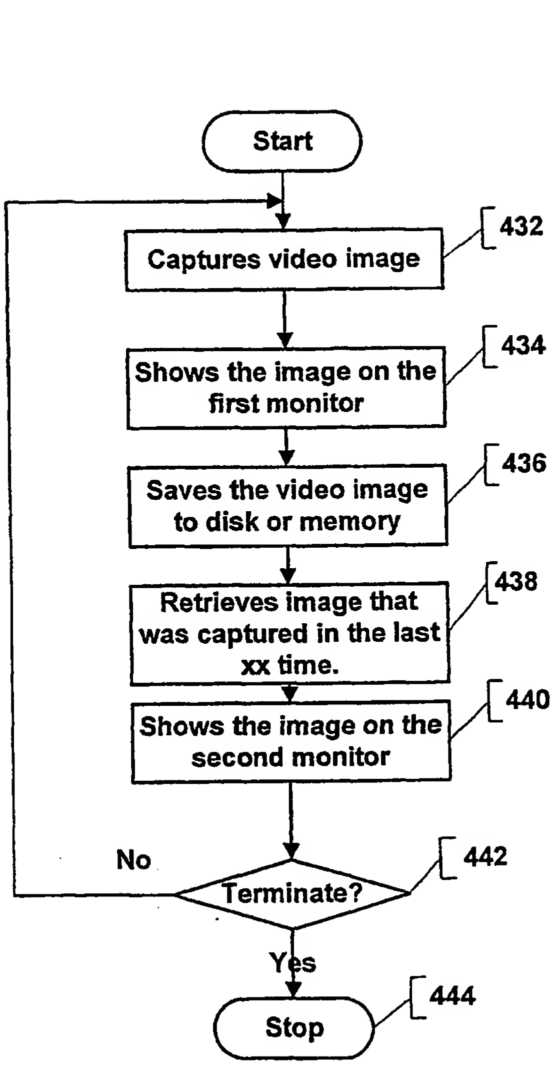

430
Start
Captures video image
432
Shows the image on the first monitor
434
Saves the video image to disk or memory
436
Retrieves image that was captured in the last xx time.
438
Shows the image on the second monitor
440
No
Terminate?
442
Yes
Stop
444

Figure 29

446

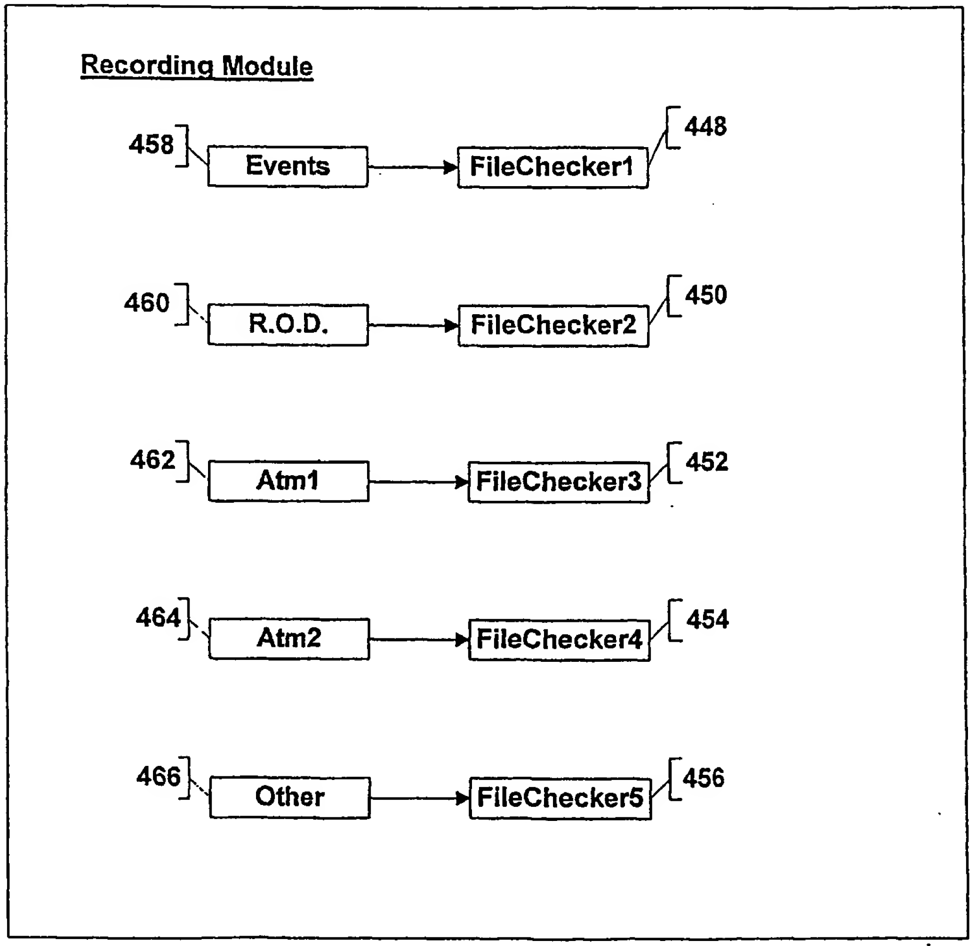


Figure 30

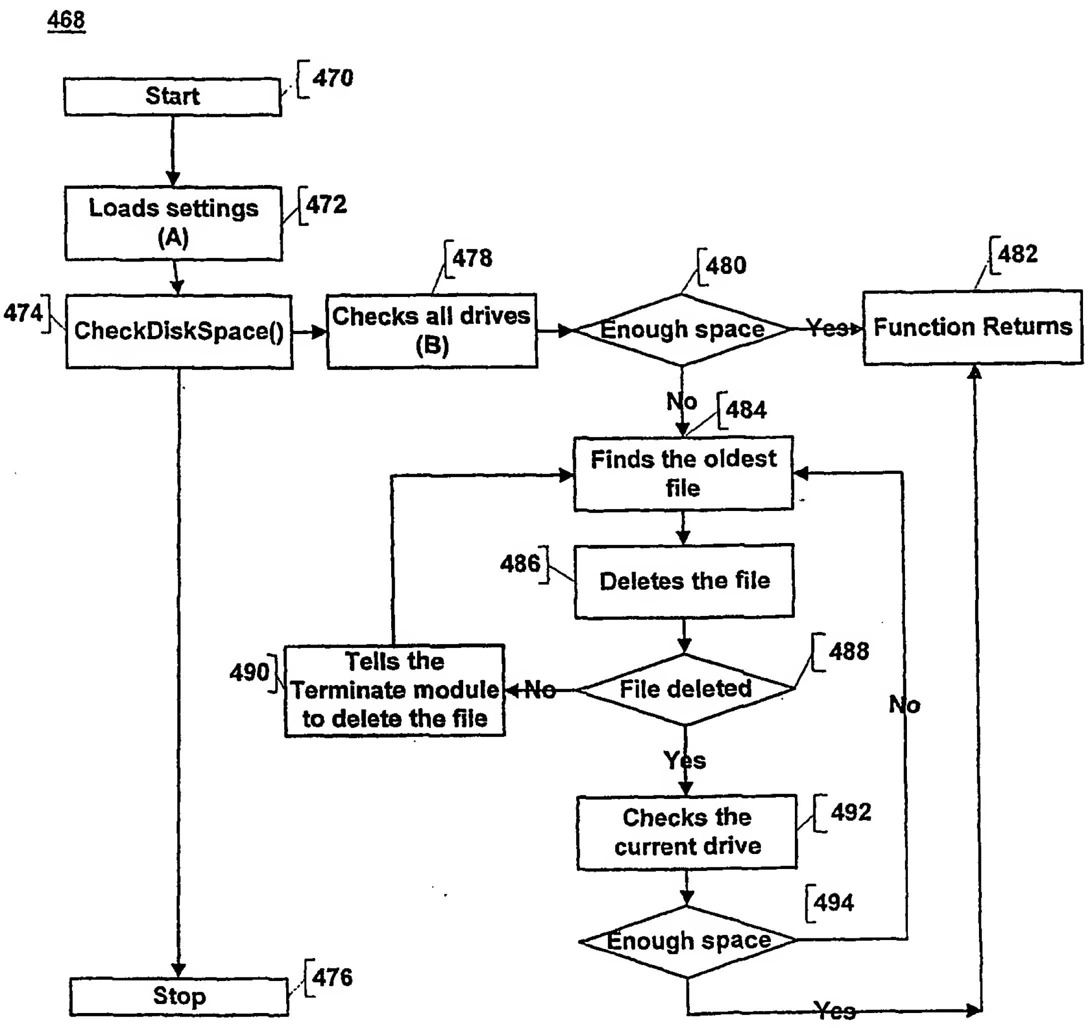

468
Start
470
Loads settings (A)
472
474
CheckDiskSpace()
Checks all drives (B)
478
Enough space
480
Yes
Function Returns
482
No
484
Finds the oldest file
486
Deletes the file
File deleted
488
No
Tells the Terminate module to delete the file
490
Yes
Checks the current drive
492
Enough space
494
No
Yes
Stop
476

Figure 31

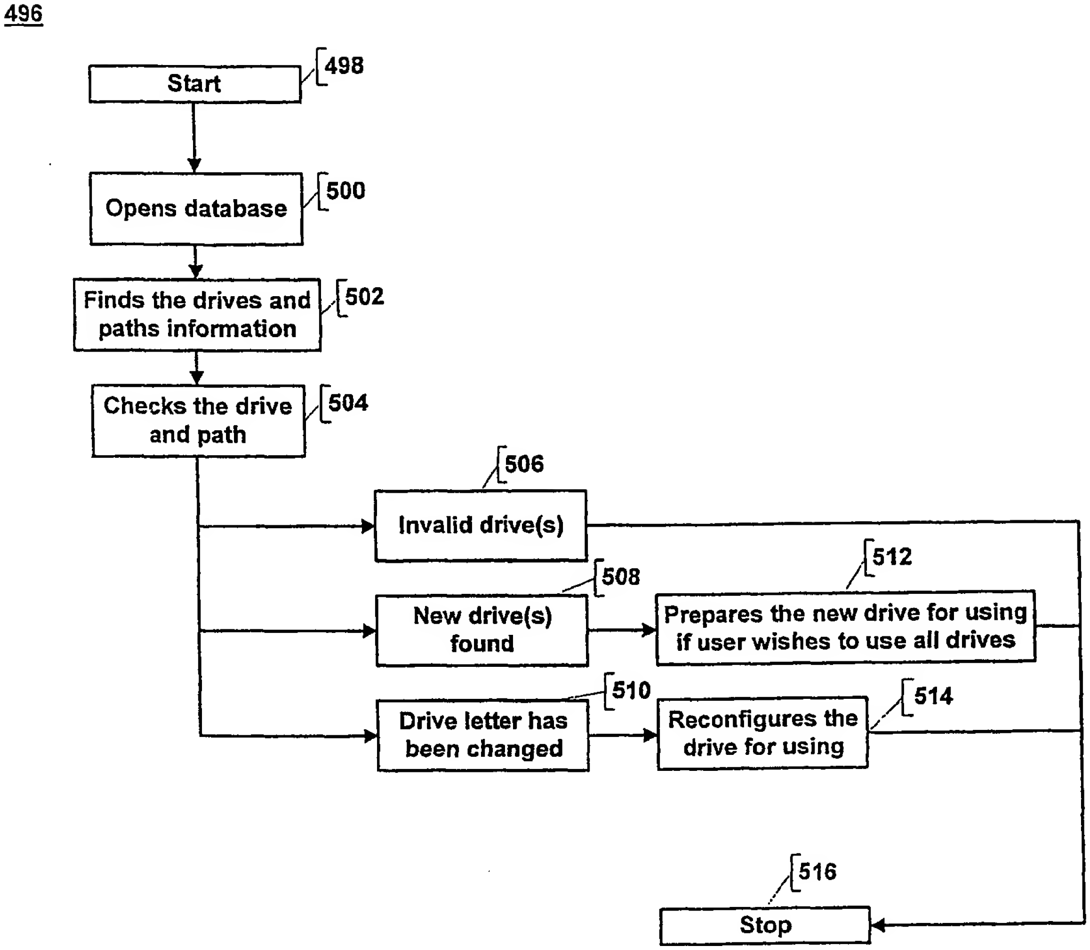

496
Start
498
Opens database
500
Finds the drives and paths information
502
Checks the drive and path
504
506
Invalid drive(s)
508
New drive(s) found
512
Prepares the new drive for using if user wishes to use all drives
510
Drive letter has been changed
514
Reconfigures the drive for using
516
Stop

Figure 32

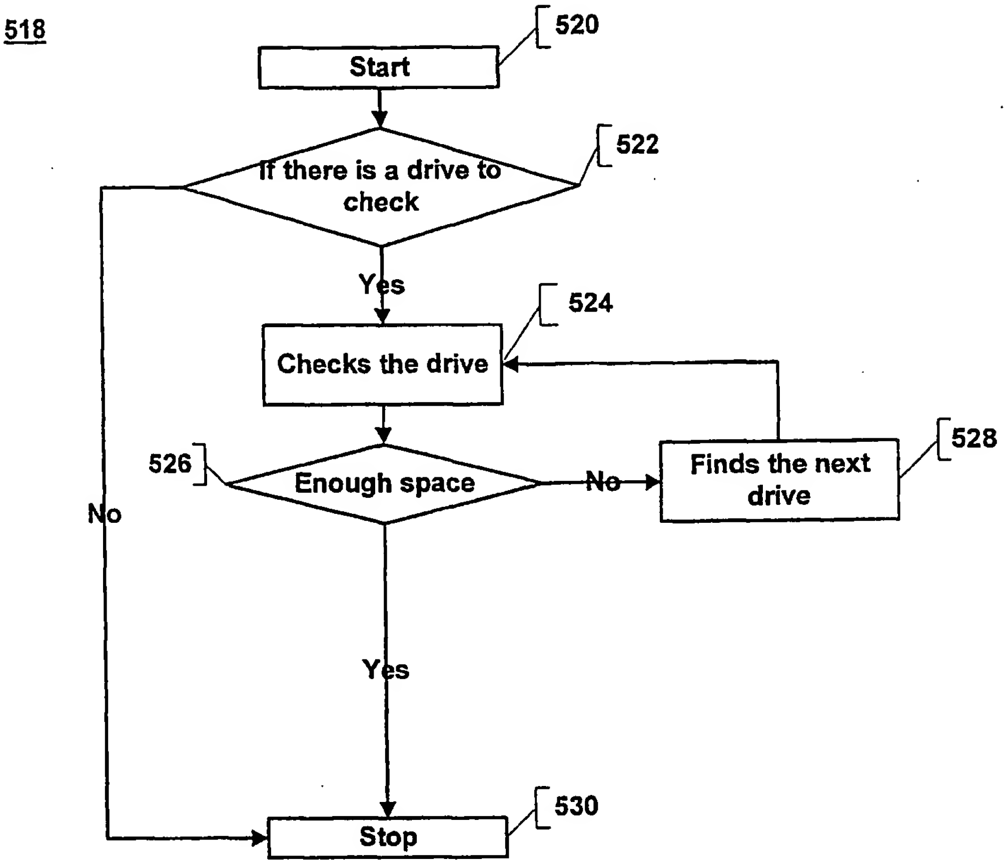

518
520
Start
522
If there is a drive to check
Yes
No
524
Checks the drive
526
Enough space
No
528
Finds the next drive
Yes
530
Stop

Figure 33

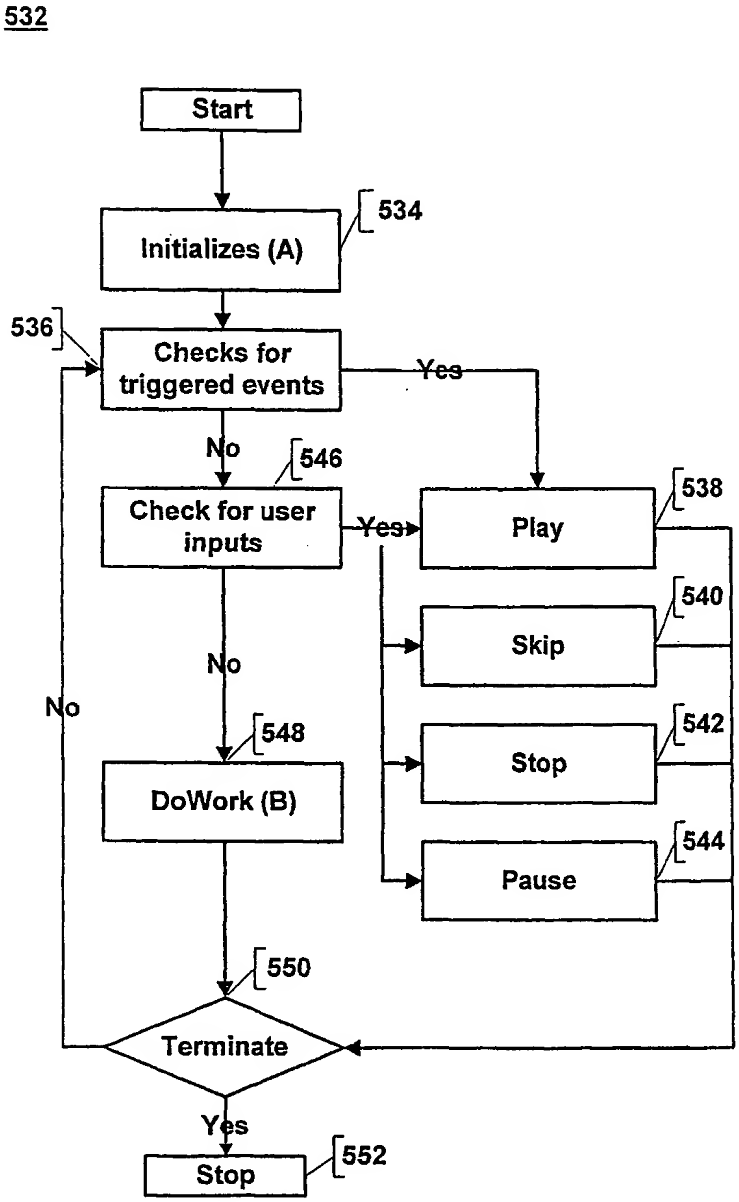

532
Start
Initializes (A)
534
536
Checks for triggered events
Yes
No
546
Check for user inputs
Yes
No
538
Play
540
Skip
542
Stop
544
Pause
No
548
DoWork (B)
550
Terminate
Yes
Stop
552

Figure 34

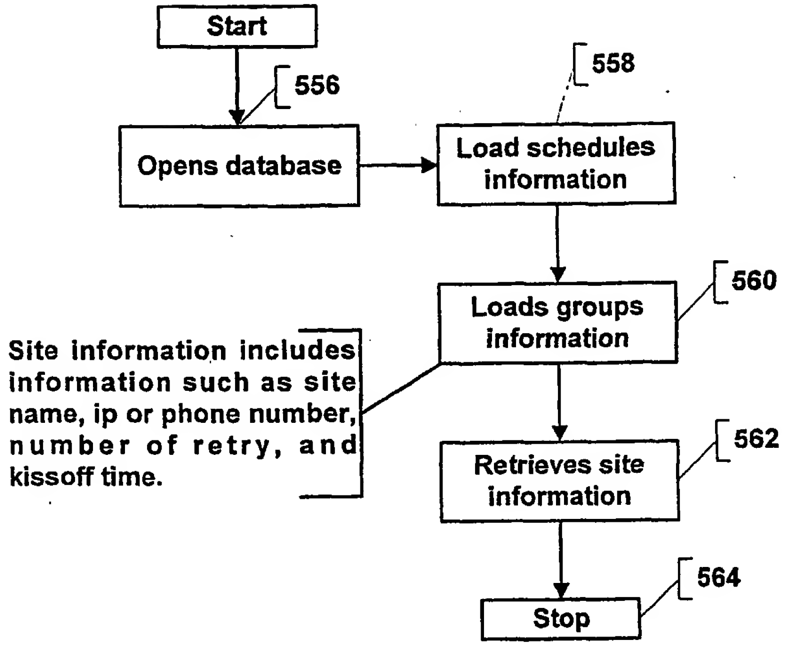
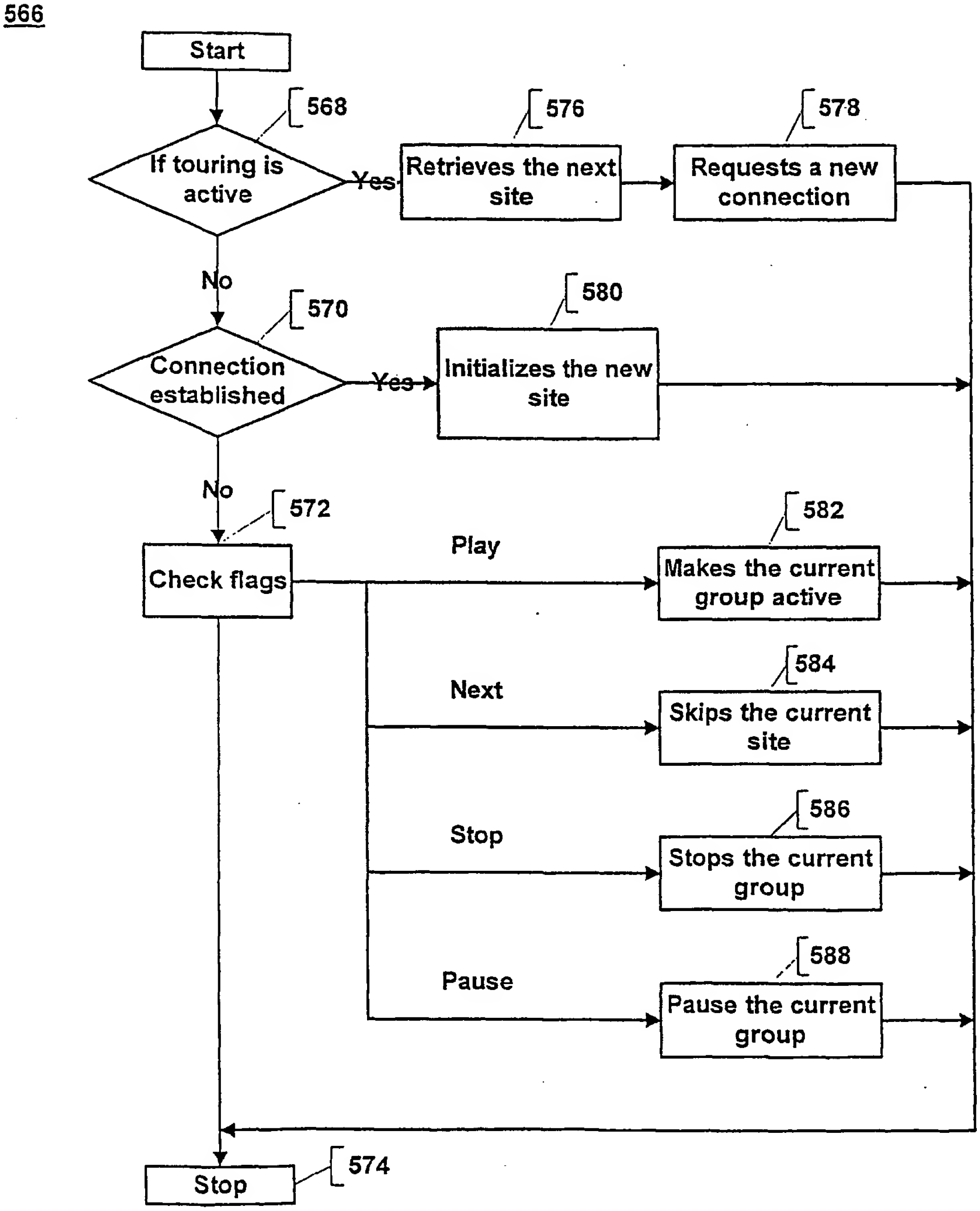

554
Start
556
Opens database
558
Load schedules information
560
Loads groups information
Site information includes information such as site name, ip or phone number, number of retry, and kissoff time.
562
Retrieves site information
564
Stop

Figure 35


566
Start
568
If touring is active
Yes
576
Retrieves the next site
578
Requests a new connection
No
570
Connection established
Yes
580
Initializes the new site
No
572
Check flags
Play
582
Makes the current group active
Next
584
Skips the current site
Stop
586
Stops the current group
Pause
588
Pause the current group
Stop
574

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/33626

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :H04M 11/04
US CL :379/44
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 379/44, 37, 38, 39, 40, 41, 42, 48, 49, 50, 93.07; 340/506, 507, 508, 524, 541; 345/507; 348/143, 152, 153, 154, 155; 358/403, 404

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

NONE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

NONE

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X ----- Y	GB 2,258,579 A (TANAKA et al.) 10 February 1993, pages 4-13.	1-4, 6, 12-13, 18, 20-21, 29-33, 38, 40-41, 48-49 ---------- 5, 7-11, 14-17, 19, 22-28, 34-37, 39, 42-47
Y	US 5,915,069 A (NISHIJIMA et al.) 22 June 1999, col. 3 line 1 through col. 4 line 27.	14-17, 24-25, 34-37, 44-45
Y	US 4,692,742 A (RAIZEN et al.) 08 September 1987, col. 4 lines 38-58 and col. 5 lines 36-42.	19, 22-23, 39, 42-43

☒ Further documents are listed in the continuation of Box C. □ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search

13 FEBRUARY 2001

Date of mailing of the international search report

11 APR 2001

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
CURTIS A. KUNTZ
Telephone No. (703) 305-4708

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/33626

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,917,409 A (WANG et al.) 29 June 1999, abstract.	26, 46
Y	US 5,251,297 A (TAKAYANAGI) 05 October 1993, abstract.	27-28, 47